North West Leicestershire District Council

Scan the code above or visit www.nwleics.gov.uk/meetings for a full copy of the agenda.

Meeting	**CABINET**
Time/Day/Date	5.00 pm on Tuesday, 20 October 2020
Location	Remote meeting using Microsoft Teams
Officer to contact	Democratic Services (01530 454512)

AGENDA

Item		Pages
1.	**APOLOGIES FOR ABSENCE**	
2.	**DECLARATION OF INTERESTS**	
	Under the Code of Conduct members are reminded that in declaring disclosable interests you should make clear the nature of that interest and whether it is pecuniary or non-pecuniary.	
3.	**PUBLIC QUESTION AND ANSWER SESSION**	
4.	**MINUTES**	
	To confirm the minutes of the meeting held on 29 September 2020	**3 - 8**
5.	**MINISTRY OF HOUSING, COMMUNITIES AND LOCAL GOVERNMENT - CONSULTATION ON PLANNING FOR THE FUTURE WHITE PAPER**	
	Report of the Strategic Director of Place Presented by the Planning and Infrastructure Portfolio Holder	**9 - 36**
6.	**LOCAL PLAN REVIEW – DRAFT OBJECTIVE 4 (SUSTAINABLE TRANSPORT)**	
	Report of the Strategic Director of Place Presented by the Planning and Infrastructure Portfolio Holder	**37 - 40**
7.	**FOOD SAFETY SERVICE DELIVERY PLAN 2020/21**	
	Report of the Strategic Director of Place Presented by the Community Services Portfolio Holder	**41 - 72**

8. REVIEW OF CORPORATE GOVERNANCE POLICIES

Report of the Chief Executive **73 - 232**
Presented by the Corporate Portfolio Holder

9. EXCLUSION OF PRESS AND PUBLIC

The officers consider that the press and public should be excluded during consideration of the following items in accordance with Section 100(a) of the Local Government Act 1972 as publicity would be likely to result in disclosure of exempt or confidential information. Members are reminded that they must have regard to the public interest test and must consider, for each item, whether the public interest in maintaining the exemption from disclosure outweighs the public interest in making the item available.

10. PAYROLL PROVISION SOFTWARE - AWARD OF CONTRACT IN EXCESS OF 5 YEARS

Report of the Strategic Director of Housing and Customer Services **233 - 238**
Presented by the Corporate Portfolio Holder

Circulation:

Councillor R Blunt (Chairman)
Councillor R Ashman (Deputy Chairman)
Councillor R D Bayliss
Councillor T Gillard
Councillor N J Rushton
Councillor A C Woodman

MINUTES of a meeting of the CABINET held in the Remote meeting using Microsoft Teams on TUESDAY, 29 SEPTEMBER 2020

Present: Councillor R Blunt (Chairman)

Councillors R Ashman, R D Bayliss, T Gillard, N J Rushton and A C Woodman

In Attendance: Councillors J Legrys

Officers: Mrs B Smith, Mr J Arnold, Mr A Barton, Mrs T Bingham, C Colvin, Mr T Delaney, Mr C Elston, Mrs M Long and Miss E Warhurst

17. APOLOGIES FOR ABSENCE

No apologies for absence were received.

18. DECLARATION OF INTERESTS

No interests were declared.

19. PUBLIC QUESTION AND ANSWER SESSION

No members of the public had requested to speak at the meeting.

20. MINUTES

Consideration was given to the minutes of the meeting held on 23 July 2020.

It was moved, seconded and

RESOLVED THAT:

The minutes of the meeting held on 23 July 2020 be approved as a correct record.

Reason for decision: To comply with the Constitution.

21. COUNCIL DELIVERY PLAN 2020/21 FORMAL ADOPTION, 2019/20 Q4 & 2020/21 Q1 MONITORING

The Leader presented the report to Cabinet and invited questions and comments from Members. It was noted that this report had been considered at a recent meeting of the Corporate Scrutiny Committee and the comments from this meeting had been taken on board.

The recommendations as set out on page 13 of the agenda were moved by Councillor Blunt, seconded by Councillor Woodman and subsequently

RESOLVED THAT:

(1) The comments of the Corporate Scrutiny Committee, as set out in annex A to the report regarding the Council Delivery Plan and performance reporting, be noted;

(2) The Council Delivery Plan, as set out in Annex B to the report, be agreed and recommended for adoption by Council;

(3) The performance reporting for Quarter 4 2019/20 and Quarter 1 2020/21, as set out in Annex C to the report, be noted.

Reason for decision: To ensure that the council has a Delivery Plan in place for the current year in line with the constitution.

22. MINISTRY OF HOUSING, COMMUNITIES AND LOCAL GOVERNMENT CHANGES TO THE CURRENT PLANNING SYSTEM: CONSULTATION ON CHANGES TO PLANNING POLICY AND REGULATIONS

Councillor Robert Ashman presented the report to Cabinet. It was acknowledged that the report had been considered at some length by the Local Plan Committee.

Councillor Legrys had requested and received the permission of the Leader to speak at the meeting on this matter. Councillor Legrys set out some concerns he had with some aspects of the paper but thanked the Planning Officers for their well written report which comprised honest responses to some difficult issues.

The Leader thanked Councillor Ashman for his report and Councillor Legrys for his comments.

The recommendation as set out on page 88 of the agenda was moved by Councillor Ashman, seconded by Councillor Bayliss and subsequently

RESOLVED THAT:

Cabinet responds to the consultation in respect of changes to the current planning system, as set out in Appendix A to the report.

Reason for decision: To determine the Council's response to the consultation.

23. REVIEW OF MEDIUM TERM FINANCIAL PLAN

Councillor Nick Ruston presented the report to Cabinet.

The Leader thanked Councillor Rushton and invited questions and comments from Members. Cabinet fully supported the recommendations and expressed their thanks for all the hard work of the Finance Team which has put this Council in a much better financial position than others in the county with the additional challenge of having had no increase to the level of council tax for 12 years.

The recommendations as set out on page 114 of the agenda were moved by Councillor Rushton, seconded by Councillor Gillard and subsequently

RESOLVED THAT:

(1) The Council's revised Medium Term Financial Plans be noted;

(2) The allocation in principle of £100k from the self-sufficiency reserve to engage external expertise to support the delivery of journey to self-sufficiency savings, be approved.

Reason for decision:To ensure Cabinet are fully brief on the revised Medium Term Financial Plans and resultant 5 year financial outlook before the budget for 2021 and beyond is developed.

24. PROVISIONAL FINANCIAL OUTTURN 2019/20

Councillor Nick Ruston presented the report to Cabinet.

The Leader thanked Councillor Rushton and invited questions and comments from Members. Again, thanks were extended to the Finance Team for their professionalism and hard work.

The recommendation as set out on page 133 of the agenda was moved by Councillor Rushton, seconded by Councillor Ashman and subsequently

RESOLVED THAT:

The financial performance for 2019/20, including the impact on reserves and balances as at 31 March 2020, be approved.

Reason for decision: Requirement of Financial Procedure Rules.

25. NEW AFFORDABLE HOUSING SUPPLY STRATEGY 2020

Councillor Roger Bayliss presented the report to Cabinet.

The Leader thanked Councillor Bayliss and invited questions and comments from Members. Cabinet fully supported the recommendations.

The recommendations, as set out on page 145 of the agenda, were moved by Councillor Bayliss, seconded by Councillor Gillard and subsequently

RESOLVED THAT:

(1) The Affordable Housing Supply Strategy be approved for adoption;

(2) Authority be delegated to the Head of Housing, in consultation with the portfolio holder for Housing, Property and Customer Services to make minor changes, as necessary in future, for the practical application of the Strategy.

Reason for decision: To identify the Council's priorities in relation to new affordable housing and to support the priority that Local people live in high quality, affordable homes.

26. PROCUREMENT OF HOUSING NEW BUILD CONTRACTOR

Councillor Roger Bayliss presented the report to Cabinet.

The Leader thanked Councillor Bayliss and invited questions and comments from Members. Cabinet fully supported the recommendations.

The recommendations as set out on page 185 of the agenda were moved by Councillor Bayliss, seconded by Councillor Ashman and subsequently

RESOLVED THAT:

(1) Cabinet approves the procurement of (a) construction contractor(s) for the duration of the current 3 year proposed new build programme;

(2) Authority be delegated to the Strategic Director of Housing and Customer Services in consultation with the Section 151 Officer and relevant portfolio holder to select contractors, as necessary, to deliver the programme through legally compliant framework/dynamic purchasing systems.

Reason for decision: To allow the Council to be compliant with the Procurement Rules within the Constitution.

27. MINUTES OF THE COALVILLE SPECIAL EXPENSES WORKING PARTY

Councillor Andrew Woodman presented the report to Cabinet.

The Leader thanked Councillor Woodman and invited questions and comments from Members. Thanks were extended to the members of the Coalville Special Expenses Working Party for their work; and the recommendations were welcomed.

The recommendation as set out on page 193 of the agenda was moved by Councillor Woodman, seconded by Councillor Rushton and subsequently

RESOLVED THAT:

The recommendations made by the Coalville Special Expenses Working Party, as detailed within the minutes, be noted, and that the recommendations as summarised at paragraph 3.0 be approved.

Reason for decision: To consider the recommendations made by the Coalville Special Expenses Working Party.

28. PROCUREMENT EXEMPTION IN RELATION TO THE COUNCILS DOG WARDEN AND KENNELLING SERVICES

Councillor Andrew Woodman presented the report to Cabinet.

The Leader thanked Councillor Woodman and invited questions and comments from Members. Cabinet fully supported the recommendations.

The recommendation as set out on page 201 of the agenda was moved by Councillor Woodman, seconded by Councillor Gillard and subsequently

RESOLVED THAT:

The exemption in relation to the award of a contract for the provision of dog warden and kennelling services be noted.

Reason for decision: The council's Financial and Contract Procedures require that exemptions be reported to Cabinet.

29. EXCLUSION OF PRESS AND PUBLIC

It was moved by Councillor Rushton, seconded by Councillor Gillard and subsequently

RESOLVED THAT:

In pursuance of Section 100A(4) of the Local Government Act 1972, the press and public be excluded from the remainder of the meeting on the grounds that the business to be transacted involves the likely disclosure of exempt information as defined in Paragraph 3 of Part 1 of Schedule 12A to the Act and that the public interest in maintaining this exemption outweighs the public interest in disclosing the information.

Reason for decision: To enable the consideration of exempt information.

30. THE RECOVERY OF OUR LEISURE CENTRES AND THE PARTNERSHIP CONTRACT WITH EVERYONE ACTIVE

Councillor Andrew Woodman presented the report to Cabinet and made reference to an update paper which had been circulated prior to the meeting.

The Leader thanked Councillor Woodman and invited questions and comments from Members. Cabinet fully supported the recommendations.

The recommendations as set out on pages 203 and 204 of the agenda were moved by Councillor Woodman, seconded by Councillor Rushton and subsequently

RESOLVED THAT:

The recommendations as set out on pages 203 and 204 of the agenda be approved.

Reason for decision: To agree a financial support package for October 2020 to March 2021 inclusive on an open book basis to continue to rebuild the community access to our leisure centres in a Covid safe environment.

31. AGILE IT EQUIPMENT SUPPLIER PROCUREMENT EXEMPTION

Councillor Roger Bayliss presented the report to Cabinet.

The recommendation as set out on page 217 of the agenda was moved by Councillor Bayliss, seconded by Councillor Gillard and subsequently

RESOLVED THAT:

The recommendation as set out on page 217 of the agenda be approved.

Reason for decision: The council's Financial and Contract Procedures require that exemptions be reported to Cabinet.

The meeting commenced at 5.00 pm

The Chairman closed the meeting at 5.43 pm

Chairman's initials

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

CABINET – TUESDAY 20 OCTOBER 2020

Title of Report	**MINISTRY OF HOUSING, COMMUNITIES AND LOCAL GOVERNMENT – CONSULTATION ON PLANNING FOR THE FUTURE WHITE PAPER**	
Presented by	Councillor Robert Ashman Planning and Infrastructure Portfolio Holder	
Background Papers	Planning for the Future – White Paper	**Public Report:** Yes **Key Decision:** Yes
Financial Implications	The proposed changes would have significant resource implications for the Council. The consultation recognises this and does refer to making additional resources available for local authorities. However, at this time the exact impact is unclear. **Signed off by the Section 151 Officer**: Yes	
Legal Implications	Although there are no legal implications with submitting comments to this consultation, the suggested changes if implemented by the Government will have legal implications. Under the current system, each local planning authority must engage with neighbouring local planning authorities under the duty to co-operate provisions set out in legislation. This places a legal duty to engage with one another in the context of strategic cross boundary development matters. In addition, local planning authorities must demonstrate how they have complied with the duty at the independent examination of their Local Plan. The proposals under the White Paper seeks to remove this duty, along with other legal tests such as the current test of soundness in preparing local plans. The proposed changes to national planning legislation will need to be examined carefully as the Council continues to prepare for the substantive review of its local plan pending these proposed changes, as well as future reviews, particularly because the NPPF would become the primary source of policies for development management in England. The suggested changes will also mean future local plans would need to be completed within 30 months. The role of planning committees would be reduced, as the proposals create a far more centralised planning system. The Council would be subject to a new performance framework which would enable earlier intervention/sanction if 'problems' emerge and deadlines set are not met. **Signed off by the Monitoring Officer**: Yes	
Staffing and Corporate Implications	The suggested changes could have implication for how the Planning service is organised and resourced. **Signed off by the Head of Paid Service:** Yes	

Purpose of Report	To consider the Government's White Paper entitled 'Planning for the future'
Reason for Decision	To determine the Council's response to the consultation.
Recommendations	**THAT CABINET RESPONDS TO THE CONSULTATION IN RESPECT OF THE PLANNING FOR THE FUTURE WHITE PAPER AS SET IN QUESTIONS 1 TO 26 ATTACHED AT APPENDIX A OF THIS REPORT.**

1. BACKGROUND

1.1 The Ministry of Housing, Communities and Local Government is seeking views on proposed changes to the planning system set out in a White Paper (Planning for the Future) which it has issued for consultation. The consultation document can be viewed here. This consultation closes on 29 October 2020.

1.2 The consultation states that the government wishes to "*undertake fundamental reform of the planning system to address its underlying weaknesses*".

1.3 To achieve this it sets out five overarching aims:

- We will streamline the planning process with more democracy taking place more effectively at the plan-making stage, and will replace the entire corpus of plan-making law in England to achieve this;
- We will take a radical, digital-first approach to modernise the planning process. This means moving from a process based on documents to a process driven by data;
- To bring a new focus on design and sustainability;
- We will improve infrastructure delivery in all parts of the country and ensure developers play their part, through reform of developer contributions; and
- To ensure more land is available for the homes and development people and communities need, and to support renewal of our town and city centres.

1.4 The consultation and the suggested response are due to be considered by the Local Plan Committee at its meeting on 15 October 2020. A copy of that report is attached at Appendix A of this report. The views of the Local Plan Committee will be reported verbally to Cabinet at its meeting.

2.0 KEY MESSAGES

2.1 The key messages from the consultation are outlined below for member's information.

Pillar one – planning for development

- Local Plans to classify land into one of three categories – growth, renewal or protected;
- Local Plans to be concerned with specific development standards with nationally set development management policies;
- Local Plans to be subject to a new test of "sustainable development" in place of the current 'soundness' test;
- Local Plans to be prepared within 30 months and one period of formal consultation;
- Further changes to the standard method for identifying housing requirements which would factor in constraints and opportunities;
- Areas identified as Growth areas would automatically be granted outline planning permission for the principle of development;
- Deadlines for determining planning applications should be firmer with potential penalties for not adhering to them;
- Greater use of digital technology for both plan-making and planning applications.

Pillar two – planning for beautiful and sustainable places

- Binding design guidance and codes to be prepared locally with community involvement;
- A body to be established to support the delivery of provably locally-popular design codes, and propose that each authority should have a chief officer for design and place-making;
- A fast track system to be introduced for beauty and more use of Pattern Books to enable popular and replicable forms of development to be approved easily and quickly;
- Introduction of a simplified method for assessing the environmental impact of proposals.

Pillar three – planning for infrastructure and connected places

- Abolition of planning obligations (S106 Agreements) and Community Infrastructure Levy and replacement with nationally set levy;
- The new levy to be expanded to also includes developments done as permitted development;
- The levy to ensure the delivery of affordable housing;
- Potentially freedom for how authorities use monies raised under the levy.

Policies and other considerations, as appropriate	
Council Priorities:	- Supporting Coalville to be a more vibrant, family-friendly town - Support for businesses and helping people into local jobs - Developing a clean and green district - Local people live in high quality, affordable homes - Our communities are safe, healthy and connected
Policy Considerations:	The proposals outlined in the consultation have the potential to have a fundamental impact upon the Council's Local Plan, which is currently being reviewed.
Safeguarding:	None identified at this time
Equalities/Diversity:	Some aspects of the proposals set out in the White Paper have a potential to have a negative impact upon some sectors of the community. For example, the greater use of digital technology could impact those without access to computers and so prohibit their participation in the planning system. Furthermore if proposals relating to affordable housing shift the role of specifying the affordable housing contribution in favour of the developer there is a risk that specialist provision will be reduced impacting on groups with protected characteristics.
Customer Impact:	No issues identified
Economic and Social Impact:	No specific issues identified, but see comments under policy considerations and risks
Environment and Climate Change:	No specific issues identified, but see comments under policy considerations and risks
Consultation/Community Engagement:	None

Risks:	The proposals set out in the White Paper would have significant resource implications for the Council. Depending upon the timing of any changes, there could be an impact upon the Local Plan review in terms of its scope, content and look. If transition arrangements are not put in place or are not robust, there is a risk that current work on the review could be jeopardised or lost. This matter will need to be kept under review.
Officer Contact	Ian Nelson Planning Policy Team Manager 01530 454677 ian.nelson@nwleicestershire.gov.uk

APPENDDIX A

LOCAL PLAN COMMITTEE – THURSDAY 15 OCTOBER 2020

Title of Report	**MINISTRY OF HOUSING, COMMUNITIES AND LOCAL GOVERNMENT – CONSULTATION ON PLANNING FOR THE FUTURE WHITE PAPER**	
Presented by	Ian Nelson Planning Policy Team Manager	
Background Papers	Planning for the Future – White Paper	**Public Report:** Yes **Key Decision:** Yes
Financial Implications	The proposed changes would have significant resource implications for the Council. The consultation recognises this and does refer to making additional resources available for local authorities. However, at this time the exact impact is unclear. **Signed off by the Section 151 Officer**: Yes	
Legal Implications	Although there are no legal implications with submitting comments to this consultation, the suggested changes if implemented by the Government will have legal implications. Under the current system, each local planning authority must engage with neighbouring local planning authorities under the duty to co-operate provisions set out in legislation. This places a legal duty to engage with one another in the context of strategic cross boundary development matters. In addition, local planning authorities must demonstrate how they have complied with the duty at the independent examination of their Local Plan. The proposals under the White Paper seeks to remove this duty, along with other legal tests such as the current test of soundness in preparing local plans. The proposed changes to national planning legislation will need to be examined carefully as the Council continues to prepare for the substantive review of its local plan pending these proposed changes, as well as future reviews, particularly because the NPPF would become the primary source of policies for development management in England. The suggested changes will also mean future local plans would need to be completed within 30 months. The role of planning committees would be reduced, as the proposals create a far more centralised planning system. The Council would be subject to a new performance framework which would enable earlier intervention/sanction if 'problems' emerge and deadlines set are not met. **Signed off by the Monitoring Officer**: Yes	
Staffing and Corporate Implications	The suggested changes could have implication for how the Planning service is organised and resourced. **Signed off by the Head of Paid Service:** Yes	
Purpose of Report	To consider the Government's White Paper entitled 'Planning for the future'	

Recommendations	**THAT CABINET BE ADVISED THAT THIS COMMITTEE RECOMMENDS THAT CABINET RESPONDS TO THE CONSULTATION IN RESPECT OF THE PLANNING FOR THE FUTURE WHITE PAPER AS SET OUT IN SECTIONS 3 TO 5 OF THE REPORT**

1. BACKGROUND

1.1 The Ministry of Housing, Communities and Local Government is seeking views on proposed changes to the planning system set out in a White Paper (Planning for the Future) which it has issued for consultation. The consultation document can be viewed here. This consultation closes on 29 October 2020.

1.2 The consultation states that the government wishes to "undertake fundamental reform of the planning system to address its underlying weaknesses".

1.3 To achieve this it sets out five overarching aims:

- To streamline the planning process with more democracy taking place more effectively at the plan-making stage, and will replace the entire corpus of plan-making law in England to achieve this;
- To take a radical, digital-first approach to modernise the planning process. This means moving from a process based on documents to a process driven by data;
- To bring a new focus on design and sustainability;
- To improve infrastructure delivery in all parts of the country and ensure developers play their part, through reform of developer contributions; and
- To ensure more land is available for the homes and development people and communities need, and to support renewal of our town and city centres

1.4 These aims are then supported by three pillars with each pillar the subject of a number of proposals:

- Pillar One – Planning for development (Proposals 1 to 10)
- Pillar Two – Planning for beautiful and sustainable places (Proposals 11 to 18)
- Pillar Three – Planning for infrastructure and connected places (Proposals 19 to 24)

1.5 There are a series of questions throughout the consultation document which largely relate to the actual proposals, although some of the proposals are not subject to a specific question. A number of questions (for examples questions 1 to 4 – see Appendix A) appear to be aimed more at members of the public rather than local authorities or other institutions. Therefore, no response is proposed to these questions in this report. Should members want a reply to these questions be included then they should advise officers of the suggested response.

1.6 Section 2 provides an over view of why the government considers that reform is required.

1.7 Sections 3 to 5 this report provide an outline of the various proposals. The box after each proposal sets out the specific questions and the suggested response (in bold).

1.8 As this is a White Paper it is inevitable that there is a lack of detail. This does make responding quite difficult as ultimately it is the details which will determine whether the proposals are successful or not. For this reason, a number of the questions are responded to with a 'not sure'.

2.0 WHY IS REFORM NEEDED

2.1 The consultation identifies that the government considers that reform of the planning system is needed because:

- It is too complex;
- Decisions are discretionary rather than rules based;
- It takes too long to adopt a Local Plan;
- Assessments of housing need, viability and environmental impacts are too complex and opaque;
- It has lost public trust;
- It is based on 20th-century technology;
- The process for negotiating developer contributions to affordable housing and infrastructure is complex;
- There is not enough focus on design, and little incentive for high quality new homes and places;
- It does not lead to enough homes being built.

3.0 PILLAR ONE – PLANNING FOR DEVELOPMENT

3.1 A new approach to plan making

3.1.1 Proposal 1: The role of land use plans should be simplified (question 5)

New local plans will be required to designate land into one of three categories:

- Growth, suitable for "substantial development" the meaning of which would be defined in policy “to remove any debate about this descriptor”. It would include urban extensions, new settlements and areas for redevelopment. A site included in this category would have outline approval for development (further information on this is included under Proposal 5).
- Renewal, suitable for "development including gentle densification and infill of residential areas, development in town centres, and development in rural areas that is not identified as Growth or Protected areas.
- Protected, this would include sites and areas which, as a result of their particular environmental and/or cultural characteristics, would justify more stringent development controls to ensure sustainability (e.g. Areas of Outstanding Natural Beauty, Conservation Areas, Local Wildlife Sites and important areas of green space). The text suggests that some development might still be ‘permissible’.

The consultation suggests that an alternative approach would be to limit permission in principle to areas identified for substantial growth (i.e. growth areas).

5. Do you agree that Local Plans should be simplified in line with our proposals?
[Yes / No / Not sure. Please provide supporting statement.]

No.

The proposed approach is too simplistic. Dividing all land into areas implies that impacts can be neatly contained in their respective areas. However, land types do not respect natural boundaries. For example, nature, and the wider environment are cross-boundary matters and do not sit neatly within such a rigid approach. How will wildlife and the natural environment be protected when it is located outside a 'protected' area? The approach potentially conflicts with the Environment Bill's proposals on biodiversity net gain and improvement plans.

Such an approach also does not provide sufficient flexibility to deal with changing circumstances. For example, if an area is identified as being Protected but a major proposal arises for the creation of a significant number of new and well paid jobs as a result of inwards investment, then such a proposal could not be supported,

unless the policy pertaining to the Protected area allowed for such circumstances in which case how is this different to the current approach?

It is not clear as to whether Protected Areas could include areas within an otherwise Growth Area. It is noted that some Protected Areas would be defined nationally and some locally, but there is a lack of clarity as to how such areas would be defined or what flexibility there would be for local authorities in defining such areas. The term 'Protected' could be misleading if some form of development is to be allowed and so an alternative form of wording might be appropriate.

In Growth Areas it would be necessary to try and envisage all the different types of development that would be appropriate and how they would need to look. This could lead to long and unwieldy Design Codes or Masterplans. It is difficult to see how such a level of detail could be achieved within the local plan process itself, given the proposed new time limit and the emphasis on front-end community engagement. To reconcile with the time limits suggested in the consultation it may be necessary to minimise the amount of detail that Design Codes or Masterplans contain such that they would be virtually meaningless and so result in very little control over subsequent development, to the detriment of local communities.

Furthermore, it is not clear as to what the expectations would be in terms of assessing the likely environmental implications arising from a Masterplan or Design Code for development in in Growth area.

3.1.2 Proposal 2: Development management policies established at national scale and an altered role for Local Plans (question 6)

It is proposed that development management policies contained in local plans would be restricted to those that are necessary site or area-specific requirements, including broad height limits, scale and/or density limits for land included in Growth areas and Renewal areas, established through the accompanying text. The National Planning Policy Framework would become the primary source of policies for development management. Local Plans would be concerned with specific development standards.

It is proposed that the local plan would be supported by Design Guides and Codes, potentially twin tracked alongside the preparation of the local plan.

Question 6. Do you agree with our proposals for streamlining the development management content of Local Plans, and setting out general development management policies nationally? [Yes / No / Not sure. Please provide supporting statement.]

No

It is not considered that it would be possible to develop a set of national policies which would be sufficiently meaningful whilst also recognising the uniqueness of different areas. There is a risk that such policies would be so generic as to be meaningless. What is appropriate in one area of the country may not be appropriate in other areas. For example, within North West Leicestershire it would be appropriate to continue to include policies that relate to the National Forest and also the River Mease Special Area of Conservation, as these are important local considerations which could not be reflected in national policies.

3.1.3 Proposal 3: Local Plans should be subject to a single statutory "sustainable development" test, replacing the existing tests of soundness (question 7).

It is proposed:

- That this would consider whether the plan contributes to achieving sustainable development in accordance with policy issued by the Secretary of State.
- To remove the requirement for a Sustainability Appraisal and replace it with a simplified system for assessing environmental impacts and to also remove the Duty to Cooperate requirement (whilst also looking at how to ensure cross boundary strategic issues are planned for).

7(a). Do you agree with our proposals to replace existing legal and policy tests for Local Plans with a consolidated test of "sustainable development", which would include consideration of environmental impact? [Yes / No / Not sure. Please provide supporting statement.]

Not sure in the absence of details as to what the "Sustainable Development" would actually entail. The consultation document states "*The achievement of sustainable development is an existing and well-understood basis for the planning system*". However, this is misleading as sustainable development can be interpreted in many different ways. Any test would need to be absolutely clear in terms of what it entails and how it is expected that it would be assessed through the Examination process. There is a need to avoid the mistakes of the past when the Local Development Framework system was introduced and the first plans failed the test of 'Soundness', so setting back plan making.

Any proposed test needs to be subject to extensive consultation with practitioners before it is formally introduced.

7(b). How could strategic, cross-boundary issues be best planned for in the absence of a formal Duty to Cooperate?

This would need to be included as part of the "sustainable development test" with authorities being required to demonstrate that account has been taken of any cross-boundary issues, using a mechanism along the a lines of a Statement of Common Ground. There would be a need for some form of national guidance as to what constitutes a cross-boundary issue including a definition of strategic infrastructure.

3.1.4 Proposal 4: A standard method for establishing housing requirement figures which ensures enough land is released in the areas where affordability is worst, to stop land supply being a barrier to enough homes being built. The housing requirement would factor in land constraints and opportunities to more effectively use land, including through densification where appropriate, to ensure that the land is identified in the most appropriate areas and housing targets are met (question 8)

This would represent a further change to the standard method used to identify the housing requirement in a local plan, from that proposed as part of the "Changes to the Current Planning system" consultation recently considered by members.

The consultation identifies that the requirement would build in a buffer" *to account for the drop off rate between permissions and completions as well as offering sufficient choice to the market".*

Local authorities would still have the responsibility to allocate land suitable for housing.

It is suggested that the proposed approach should ensure that enough land is planned for and with sufficient certainty as to its development and so it is proposed to remove the requirement for a demonstrating 5-year supply of housing land, but the housing delivery test and the presumption in favour of sustainable development would be retained.

8(a). Do you agree that a standard method for establishing housing requirements (that

takes into account constraints) should be introduced? [Yes / No / Not sure. Please provide supporting statement.]

No

It is not clear whether the outcome form the standard method would be updated annually or would it be for a set period of time. If the latter as the outcome from this would be binding, it offers no flexibility to take account of any changes in circumstances. Either way, it represents a top down approach to planning.

Again the lack of detail regarding any proposal makes it difficult to comment. A key consideration will be what constraints are to be considered as this will impact upon the final requirement figure, but also who will be the final decision maker as to what is a constraint? Will there be consultation with authorities and other stakeholders? Furthermore, it is not clear as to whether all constraints will be given equal weighting or will some carry more weight. Again who would determine such weighting and will there be any consultation prior to a decision being made? The process for making decisions needs to be totally transparent to ensure a consistent approach across the country.

It would appear that Green Belt is being considered as sacrosanct. It is not considered that this represents a sustainable approach and would penalise those areas without Green Belt, even though it may be Green Belt authorities that have been under delivering.

8(b). Do you agree that affordability and the extent of existing urban areas are appropriate indicators of the quantity of development to be accommodated? [Yes / No / Not sure. Please provide supporting statement.]

Not sure.

More clarity is required to be better able to understand how this proposal might operate. For example, what is meant by an urban area? There needs to be a clear definition.

Whilst it is reasonable to assume that larger urban areas will generate more need, this does not mean that such areas are capable of accommodating such development.

It is not clear from the consultation as to how the affordability element is to be defined. For example, is it to be as per the recent consultation on other changes to the standard method (Changes to the current planning system) or is it to be a different approach. If the former, the Council is of the view that this gives too much weight to affordability which in itself is an extremely complex issue, not all of which is related to the availability of housing.

3.2 **A streamlined development management process with automatic planning permission for schemes in line with plans**

3.2.1 Proposal 5: Areas identified as Growth areas (suitable for substantial development) would automatically be granted outline planning permission for the principle of development, while automatic approvals would also be available for pre-established development types in other areas suitable for building (question 9).

In areas suitable for substantial development (Growth areas) an outline permission for the principle of development would be conferred by adoption of the Local Plan. Further details would be agreed and full permission achieved through streamlined and faster consent routes which focus on securing good design and addressing site-specific technical issues.

In areas suitable for development (Renewal areas), there would be a general presumption in favour of development. Consent for development would be granted in one of three ways:

- for pre-specified forms of development through a new permission route which gives an automatic consent if the scheme meets design and other prior approval requirements
- a faster planning application process where a planning application for the development would be determined in the context of the Local Plan description; or
- a Local or Neighbourhood Development Order.

Proposals in protected areas would continue to come forward as planning applications.

9(a). Do you agree that there should be automatic outline permission for areas for substantial development (Growth areas) with faster routes for detailed consent? [Yes / No / Not sure. Please provide supporting statement.]

No

It is not clear as to what would constitute "Suitable for substantial development" and nor is it clear as to how any environmental impacts are expected to be taken in to account and assessed as part of the process of identifying Growth Areas in Local Plans, particularly as it is proposed to no longer require a Sustainability Appraisal. Would a developer still be required to undertake an Environmental Impact Assessment (EIA) at the full permission stage? If so, this just means that the EIA is being done later in the process, so not saving the developer time and money. However, of more concern is what then happens if such an assessment identifies an impact which cannot be resolved but there is permission in principle for the site?

The planning process should not be based on speed at the expense of unforeseen adverse impacts and the environment, these need to be considered as part of the plan making process.

Proposal 14 in respect of a fast track for beauty suggests that site-specific codes and masterplans could be developed "*subsequent to*" the local plan being approved. However, it also states that these documents "*should be in place prior to detailed proposals coming forward*" in the area. This is a contradiction which requires clarification. It is also suggested that that masterplans could in some cases be prepared by the site promoter rather than by the local authority. This passes control from the local authority to the site promoter, but what happens if the local authority have concerns about the masterplan. Would this then be an issue to be resolved at Examination? If so it would add more time to the Examination process.

North West Leicestershire already has a Good Design Guide in place which is resulting in higher quality of developments. There is a concern that this could be diluted if control is passed to the developer.

If there is an expectation that plans include some form of masterplan, and there is also a strict timetable for preparing local plans, then these need to avoid being too detailed whilst also giving a clear indication as to what is expected.

9(b). Do you agree with our proposals above for the consent arrangements for Renewal and Protected areas? [Yes / No / Not sure. Please provide supporting statement.]

No

It is questioned as to whether it is possible to identify all the likely future uses that

could be acceptable in such areas. What might be appropriate in one area, might not be so in another area.

9(c). Do you think there is a case for allowing new settlements to be brought forward under the Nationally Significant Infrastructure Projects regime? [Yes / No / Not sure. Please provide supporting statement.]

Not sure

It is assumed that this would require the government to issue a National Policy Statement before such an approach could be taken. It is not clear as to what such a statement would say. For example, would it identify the need for a new settlement of xxxxx homes in a specific region, county or local authority area and if so how would these areas be identified? Without some form of guidance as to the number required there could be a proliferation of proposals and potentially approvals.

A further concern is how such proposals would then interface with the preparation of local plans. For example, would local plans be expected to only make a certain level of provision on the basis that a new settlement would be forthcoming?

3.2.2 Proposal 6: Decision-making should be faster and more certain, with firm deadlines, and make greater use of digital technology (question 10)

The 8 and 13-week targets for determining planning applications would remain but would be a firm deadline. This would be achieved through a number of means including greater digitisation of the application process, shorter and more standardised applications, data rich planning application registers and the possible right for refund of the application fee where an application is not determined within the specified period.

10. Do you agree with our proposals to make decision-making faster and more certain? [Yes / No / Not sure. Please provide supporting statement.]

Yes in principle. However, the desire to speed up the process for determining planning applications should not be at the expense of the quality of development that results. Therefore, it is considered that if the time limits for determining planning applications are to remain, the current system whereby both the local authority and the applicant agree extensions of time should be retained. Developers are happy with the current approach which gives flexibility and removing extension of time agreements would mean applications refused at 8 and 13 weeks just to meet a target.

If the time limits are to be firm deadlines then this needs to be balanced by the provision of powers for local authorities to be able to refuse to consider applications which are not supported by all of the necessary information. The clock should not start until all the necessary information is available to enable a decision to be fully informed.

There will also be a need to ensure that statutory consultees are sufficiently resourced and managed to ensure that they respond within any timeframes.

Consideration also needs to be given to those situations where an application has been submitted with all of the necessary supporting information, but a consultee then identifies a need for further evidence. This could potentially result in application's having to be refused merely to meet the decision deadline.

The use of more digital technology is welcomed but it should be appreciated that this will have resource implications for local authorities. Furthermore, it is important to not exclude those sections of the community who do not have access

to technology either because they cannot afford it or choose not to use it.

Simplification of the application process is in terms of shorter more standardised applications and greater standardisation of supporting information is welcomed along with setting out what the key information needs to be, but equally important is ensuring that national policy is made clear that failure to provide this information would make the application invalid.

A set of national standard conditions to cover common issues is to be encouraged providing that there is still scope for bespoke conditions to deal with site specific or locally occurring issues (such as the River Mease/National Forest in NWLDC).

The delegation of detailed planning decisions to planning officers would speed up decision making but would be at the detriment to local democracy as a local ward councillor /community would no longer be able to request that applications are heard at Planning Committee. Planning Committee members and the local community will almost certainly feel that their views are being marginalised. Therefore locally agreed call in procedures should continue to be supported.

3.3 **A new interactive, web-based standard for planning documents**

3.3.1 Proposal 7: Local Plans should be visual and map-based, standardised, based on the latest digital technology, and supported by a new template (question 11).

Local plans would be web-based and interactive, supported by a more limited evidence base and there would be a model template for local plans. They should be accessible in different formats and on different devices. The consultation suggest that this could transform how communities engage with local plans, including making it more likely that younger people would engage.

11. Do you agree with our proposals for accessible, web-based Local Plans? [Yes / No / Not sure. Please provide supporting statement.]

Yes

The use of more digital technology is welcomed but it should be appreciated that this will have resource implications for local authorities. Furthermore, it is important to not exclude those sections of the community, including small Parish Councils/meetings who do not have access to technology either because they cannot afford it or choose not to use it.

On the basis of what is suggested in the consultation it would appear that the intention is to have greater standardisation between local authorities' local plans. It is not clear what room this would leave for local distinctiveness.

3.4 **A streamlined, more energising plan-making process**

3.4.1 Proposal 8: Local authorities and the Planning Inspectorate will be required through legislation to meet a statutory timetable for key stages of the process, and we will consider what sanctions there would be for those who fail to do so (question 12).

Local plans would be required to be produced in 30 months with 5 stages:

- Stage 1 – (6 months) local authority "calls for" suggestions for areas under the three categories of land for where development should go and what it should look like.

- Stage 2 – (12 months): The local planning authority draws up its proposed Local Plan, and produces any necessary evidence to inform and justify the plan. "Higher-risk" authorities will receive mandatory Planning Inspectorate advisory visits, in order to ensure the plan is on track prior to submission.
- Stage 3 - (6 weeks): The local planning authority simultaneously
  (i) submits the Plan for Examination; and
  (ii) publicises the plan for the public to comment on.
- Stage 4 - (9 months): A planning inspector considers whether the three categories shown in the proposed Local Plan are "sustainable" as per the statutory test and makes binding changes which are necessary to satisfy the test
- Stage 5 - (6 weeks): Local Plan map and key are finalised and bought in to force.

12. Do you agree with our proposals for a 30 month statutory timescale for the production of Local Plans? [Yes / No / Not sure. Please provide supporting statement.]

No.

It must be recognised that in the real world there are many factors beyond the local authority's control. For example, changes in government policy or new evidence which needs to be taken in to account. There may be instances when a statutory consultee fails to provide advice within a reasonable timescales. In such circumstances local authorities would be faced with a difficult choice – carry on and risk plan not being considered acceptable or delay and some form of unknown sanctions? Local authorities (and more importantly local communities) should not be punished for failing to keep to a timetable that has been imposed on them but over which they do not have complete control.

Binding Inspector's Reports means that there is a lack of local control and power.

The proposed process only incudes one opportunity for public consultation and this is at a stage where the local authority has set out what are, in effect, its final proposals for the future development of an area. This is too late in the process to shape the authority's approach. Furthermore, it is likely that it will lead to the submission of a substantial number of comments which will then require more Exanimation time and put more pressure on the Planning Inspector.

The suggested timeframe for preparation of a Local Plan is unbalanced. For example, it is not considered proportionate to have half as much time at examination (9 months) as preparation (18 months – including call for sites). As with determining planning applications, speed should not be at the expense of quality.

3.4.2 Proposal 9: Neighbourhood Plans should be retained as an important means of community input, and we will support communities to make better use of digital tools (question 13)

Proposed that consideration be given to whether neighbourhood plan content should become more focused to reflect the proposals for Local Plans. Also proposed to consider whether there is scope to extend and adapt the concept so that very small areas – such as individual streets – can set their own rules for the form of development which they are happy to see.

13(a). Do you agree that Neighbourhood Plans should be retained in the reformed planning system? [Yes / No / Not sure. Please provide supporting statement.] 13(b). How can the neighbourhood planning process be developed to meet our objectives, such as in

the use of digital tools and reflecting community preferences about design?

Yes it is agreed that Neighbourhood Plans should continue to be retained and form part of the development plan for an area. However, many of the proposals set out in the consultation are at odds with localism and there are concerns that the proposal to introduce national policies in respect of design and development management will remove much of the scope for encouraging a truly local approach to design issues and so undermine neighbourhood plans.

13(b). How can the neighbourhood planning process be developed to meet our objectives, such as in the use of digital tools and reflecting community preferences about design?

There is no doubt that digital tools have the potential to assist neighbourhood plan groups, but only if they are made available to all at no cost and able to be used on home computers without expensive software packages. There will also need to be support available to deal with any queries or problems. To ensure that design is addressed in neighbourhood plans there would be merit in publishing guidance to help groups, such as that which was published when the then Countryside Commission introduced Village Design Statements.

3.5 **Speeding up the delivery of development**

3.5.1 Proposal 10: A stronger emphasis on build out through planning (question 14)

No specific proposals are set out at this stage, beyond proposing to make it clear through the NPPF that masterplans and design codes (see Pillar Two) should seek to include a variety of development types by different builders which allow more phases to come forward together and that further options to explore faster build out are being explored

14. Do you agree there should be a stronger emphasis on the build out of developments? And if so, what further measures would you support? [Yes / No / Not sure. Please provide supporting statement.]

Yes in principle, but local authorities need to be provided with the necessary powers and tools to ensure that development does proceed at a suitable pace. Possible measures could include a consideration of the track record of a developer in terms of delivery when determining planning applications and appeals. Alternatively, there could be an uplift to any payments due under an infrastructure levy if development does not proceed in accordance with agreed schedules.

4.0 PILLAR TWO - PLANNING FOR BEAUTIFUL AND SUSTAINABLE PLACES

4.1 **Creating frameworks for quality**

15. What do you think about the design of new development that has happened recently in your area? [Not sure or indifferent / Beautiful and/or well-designed / Ugly and/ or poorly-designed / There hasn't been any / Other – please specify]

Since 2008, North West Leicestershire District Council has invested considerable time and effort into improving design quality across our district including employing an Urban Designer to help improve design quality. It is considered that there is a far higher standard of design in the district by virtue of the Councils adopted Supplementary Design Guidance "Good Design in North West Leicestershire" and the continued commitment of officers and members. There is a strong policy framework and, in the case of residential development, a link to

using Building for Life12 to engage in the delivery of proposals.

16. Sustainability is at the heart of our proposals. What is your priority for sustainability in your area? [Less reliance on cars / More green and open spaces / Energy efficiency of new buildings / More trees / Other – please specify]

All of these to some degree. The council has declared a Climate Emergency and has also developed a Zero Carbon Roadmap with the aim of being a Net Zero Carbon Council by 2030 and a Net Zero Carbon district by 2050. Alongside a focus on renewable energy, buildings and transport are also both key sustainability work streams. With housing our focus is on driving the energy efficiency of new builds and developing an effective retrofit programme to improve standards across existing building stock. With transport it is about driving a reduction in usage through building greater connectivity across our district and promoting walking, cycling, public transport and cleaner vehicles (eg EVs). The Council's Design Guidance emphasises the importance of open spaces and tree planting, reflecting the districts location as part of the National Forest.

4.1.1 Proposal 11: To make design expectations more visual and predictable, we will expect design guidance and codes to be prepared locally with community involvement, and ensure that codes are more binding on decisions about development (question 17).

It is proposed that design guidance and codes should only be given weight in the planning process if it can be demonstrated that they have been prepared with community input. Where this is the case, the consultation states that "*we will also make clear that decisions on design should be made in line with these documents*".

17. Do you agree with our proposals for improving the production and use of design guides and codes? [Yes / No / Not sure. Please provide supporting statement.]

Not sure

It is considered that Design Codes are an essential part of helping to ensure design quality. However, there can still be quite a variation in interpretation of a code, which depends both on the quality of the document and also the aspiration and intent of the user.

There needs to clarity as to what the threshold will be for community involvement (and indeed what the definition of community might be). Will these need to be 'signed off' by the community or is it sufficient to show that the community have been given an opportunity to participate in their preparation?

One of the challenges always is to encourage a positive response to new development, which is seldom forthcoming as there is a tendency to focus on the (perceived) negative impact of development.

The preparation of a number of Design Codes will have significant resource and skill implications. It is acknowledged that this is recognised in the consultation document, but it should not be under estimated, particularly in the early years of any new processes.

4.1.2 Proposal 12: To support the transition to a planning system which is more visual and rooted in local preferences and character, we will set up a body to support the delivery of provably locally-popular design codes, and propose that each authority should have a chief officer for design and place-making (question 18).

The consultation recognises that the proposals "*set out will require a step-change in the design skills available to many local planning authorities as well as …. leadership*" and that the government will provide support. This support could include the establishment of a new expert body, possibly with a monitoring function "*performing a wider monitoring and challenge role for the sector in building better places*".

Further proposals later this year are promised for *"improving the resourcing of planning departments more broadly*".

18. Do you agree that we should establish a new body to support design coding and building better places, and that each authority should have a chief officer for design and place-making? [Yes / No / Not sure. Please provide supporting statement.]

Not sure

Whilst a design body could be a useful addition, it raises a question of its role and status and what any interrelationship might be with the Council's existing arrangements which have led to bespoke design solutions for the local area (see response to question 15). It is important that this local distinction is not lost and replaced by a more generic, centralised approach.

It would also be useful to understand what is meant by the phrase 'provably locally popular'?

The Council supports the idea to have a chief officer for design and place making.

4.1.3 Proposal 13: To further embed national leadership on delivering better places, we will consider how Homes England's strategic objectives can give greater emphasis to delivering beautiful places (question 19).

19. Do you agree with our proposal to consider how design might be given greater emphasis in the strategic objectives for Homes England? [Yes / No / Not sure. Please provide supporting statement.]

Yes

Previous experience of Homes England development in North West Leicestershire is that design was not at the heart of the process which tends to be driven more by the number of homes delivered/supported. Proposals which provide a greater emphasis on improving design quality and environmental standards in all Homes England's activities and programmes of work would be welcomed, but it must meet the Council's own requirements for design quality as et out in the Design Guidance.

4.2 **A fast-track for beauty**

4.2.1 Proposal 14: We intend to introduce a fast-track for beauty through changes to national policy and legislation, to incentivise and accelerate high quality development which reflects local character and preferences (question 20).

This builds on the work of the Building Better, Building Beautiful Commission published earlier this year. A fast-track system was one of their recommendations.

The consultation sets out 3 ways in which design quality will be enhanced:

- Changes to the NPPF;

- Legislate to require that a masterplan and site-specific code are agreed as a condition of the permission in principle which is granted through the local plan for where areas for significant development are identified;
- legislate to widen and change the nature of permitted development, so that it enables popular and replicable forms of development to be approved easily and quickly, for example through the use of Pattern Books. It appears that this would be restricted to renewal areas.

It is proposed to develop a limited set of form-based development types that allow the redevelopment of existing residential buildings where the relevant conditions are satisfied. Prior approval from the local planning authority would still be needed for aspects of the design. Local authorities and neighbourhood plans would be able to use local orders to modify how standard types apply in their areas.

20. Do you agree with our proposals for implementing a fast-track for beauty? [Yes / No / Not sure. Please provide supporting statement.]

Not sure

The term beauty is 'subjective'.

The suggested approach presupposes that the sites in Local Plans are acceptable to an Inspector. What if they are not – this would represent a waste of resources and time.

Updating the NPPF to make clear that schemes which comply with design code have more certainty would be welcomed. However, in reality it would not fundamentally change the existing system as paragraph 130 of the NPPF effectively establishes this.

There are clear resource implications for Local Authorities if they are expected to provide site-specific codes for each Growth area. It is not clear from the proposal as to whether these should be done by the Local Authority or the site promoter but providing an 'and/or' approach certainly wouldn't provide greater certainty.

It is unclear how the use of a national pattern book would foster local distinctiveness which is at the heart of the design initiative in North West Leicestershire. Instead it represents increased centralisation. The further use of permitted development rights/prior approval is at odds with the intention of creating a less complex planning system.

4.3 **Effective stewardship and enhancement of our natural and historic environment**

4.3.1 Proposal 15: We intend to amend the National Planning Policy Framework to ensure that it targets those areas where a reformed planning system can most effectively play a role in mitigating and adapting to climate change and maximising environmental benefits (no question).

The reformed planning system will continue to protect the places of environmental and cultural value which matter to people, both nationally and locally. However, the governments wants the reformed system to play a proactive role in promoting environmental recovery and long-term sustainability. A consultation on a revised NPPF in the autumn is proposed.

4.3.2 Proposal 16: We intend to design a quicker, simpler framework for assessing environmental impacts and enhancement opportunities that speeds up the process while

protecting and enhancing the most valuable and important habitats and species in England (no question).

The current frameworks for assessing the environmental impact of development (e.g. Strategic Environmental Assessment, Sustainability Appraisal, and Environmental Impact Assessment) – can lead to duplication of effort and overly-long reports which inhibit transparency and add unnecessary delays.

4.3.3 Proposal 17: Conserving and enhancing our historic buildings and areas in the 21st century (no question).

It is envisage that Local Plans will clearly identify the location of internationally, nationally and locally designated heritage assets, such as World Heritage Sites and conservation areas, as well locally important features such as protected views.

The government wants "*to explore whether there are new and better ways of securing consent for routine works, to enable local planning authorities to concentrate on conserving and enhancing the most important historic buildings. This includes exploring whether suitably experienced architectural specialists can have earned autonomy from routine listed building consents*".

4.3.4 Proposal 18: To complement our planning reforms, we will facilitate ambitious improvements in the energy efficiency standards for buildings to help deliver our world-leading commitment to net-zero by 2050 (no question).

The government will respond to the Future Homes Standard consultation it undertook earlier this year, in full in the autumn.

It is suggested that "*As local authorities are freed from many planning obligations through our reforms, they will be able to reassign resources and focus more fully on enforcement*".

5.0 PILLAR THREE – PLANNING FOR INFRASTRUCTURE AND CONNECTED PLACES

5.1 A consolidated infrastructure levy

21. When new development happens in your area, what is your priority for what comes with it? [More affordable housing / More or better infrastructure (such as transport, schools, health provision) / Design of new buildings / More shops and/or employment space / Green space / Don't know / Other – please specify]

All of these are important, but their importance will differ from site-to-site and through time. Decisions require a balanced approach in order to ensure that the overall quality of development meets the Council's aspirations.

5.1.2 Proposal 19: The Community Infrastructure Levy should be reformed to be charged as a fixed proportion of the development value above a threshold, with a mandatory nationally-set rate or rates and the current system of planning obligations abolished (question 22).

The charge would:

- be on the final value of a development based on the applicable rate at the point planning permission is granted;
- be levied at point of occupation, with prevention of occupation being a potential sanction for non-payment;
- levy set nationally but monies collected and spent locally;
- to support the timely delivery of infrastructure, local authorities allowed to borrow against Infrastructure Levy revenues to forward fund infrastructure;

- include a value-based minimum threshold below which the levy is not charged, to prevent low viability development becoming unviable, above the threshold, the Levy would only be charged on the proportion of the value that exceeded the threshold; and
- provide greater certainty for developers and communities as to what the Levy will be.

22(a). Should the Government replace the Community Infrastructure Levy and Section 106 planning obligations with a new consolidated Infrastructure Levy, which is charged as a fixed proportion of development value above a set threshold? [Yes / No / Not sure. Please provide supporting statement.]

Not sure

Such an approach has the advantage, from a local authority perspective, of potentially being simpler than either S106 agreements or the Community Infrastructure Levy. However, this would be at the expense of local ownership.

The proposal to exclude developments which are not viable from the levy should only be for a transition period as the cost of levy should be reflected in the value of the land paid by a developer. Only those sites where the land was purchased or an option agreed prior to the date on which any new levy is introduced should be eligible for an exception. Developers should be required to demonstrate that this was the case.

It is not clear as to whether the intention is that any existing S106 Agreements would remain in place until such time as all of the obligations have been discharged or would developers be able to ask to switch to the levy. Clarification is required and if this is the intention, how would any obligation discharged to date be calculated in to what would be due via a levy.

S106 Agreements also secure other contributions than those with a monetary value. For example, the provision and future management of children's play areas and open space on-site, securing sustainable travel methods and on- site community facilities (e.g. schools, doctors' surgeries). They are also used to secure mitigation which cannot be conditioned on a planning permission, such as the payment for air quality monitoring stations and the payment for ecological off-setting land. It is not clear how (or if) such contributions would be captured particularly as the consultation states that local authorities "would not be able to use Section 106 planning obligations to secure infrastructure or affordable housing".

The consultation is clear that the Infrastructure Levy is about land value capture, not mitigating specific developments. This goes against the current approach which is to ensure that otherwise acceptable development mitigates its impact. How would this approach still ensure that development did not have an unacceptable impact upon local communities?

22(b). Should the Infrastructure Levy rates be set nationally at a single rate, set nationally at an area-specific rate, or set locally? [Nationally at a single rate / Nationally at an area-specific rate / Locally]

Not sure

If a rate is to be set nationally (whether at a single rate or area specific) it is not clear as to how any local variations in cost (for example land values or build costs) would be factored in. In addition, what would be the process for setting rates, for example, would there be any consultation before confirming rates?

What measures would be put in place in terms of ensuring that any monies

raised as part of a national levy are used to address infrastructure provision in a local authority area?

If a rate is to be set locally, the process for doing so needs to be significantly simpler than that for the Community Infrastructure Levy as this has distracted from its attractiveness and deterred authorities from going down this route.

22(c). Should the Infrastructure Levy aim to capture the same amount of value overall, or more value, to support greater investment in infrastructure, affordable housing and local communities? [Same amount overall / More value / Less value / Not sure. Please provide supporting statement.]

Not sure

If the aim is to collect monies equivalent to the national level only then this will mean that some areas lose out. Therefore, as an absolute minimum any national levy should ensure that the amount collected locally is no less than that which would have been secured through S106 Agreements, including affordable housing.

22(d). Should we allow local authorities to borrow against the Infrastructure Levy, to support infrastructure delivery in their area? [Yes / No / Not sure. Please provide supporting statement.]

Not sure

It is recognised that allowing local authorities to borrow against the Infrastructure Levy could help to ensure that much needed infrastructure is provided early on in developments. However, it does represent a transfer of risk from developers to local authorities. A local authority could provide infrastructure and then for whatever reason the related development may not complete, leaving the authority with a gap in finances. There needs to be a mechanism in place to avoid this problem.

There are a number of area s which are not clear:

- **At what point can a loan could be secured. For example, would it be when permission is granted or would it be when development commences;**
- **Would the levy also allow for coverage of any interest which any loans attract, as otherwise this would be a cost to the local authority;**
- **Would this approach be compatible with State Aid rules?**

5.1.3 Proposal 20: The scope of the Infrastructure Levy could be extended to capture changes of use through permitted development rights (question 23).

This would enable additional funding to be secured from development which currently makes no contribution towards the provision of additional infrastructure, irrespective of its impact.

23. Do you agree that the scope of the reformed Infrastructure Levy should capture changes of use through permitted development rights? [Yes / No / Not sure. Please provide supporting statement.]

Yes so as to ensure that it contributes towards offsetting its potential impacts upon local communities, particularly in view of recent changes which have increased the scope of permitted development which has taken more development outside of S106 requirements. Not bringing permitted development

schemes within the scope of infrastructure contributions creates an impact upon local communities, including, amongst other things on the ability to deliver balanced communities and affordable housing.

5.1.4 Proposal 21: The reformed Infrastructure Levy should deliver affordable housing provision (question 24)

Affordable housing provision is currently secured by local authorities via Section 106 agreements, but the Community Infrastructure Levy cannot be spent on it. With Section 106 planning obligations removed, it is proposed that under the Infrastructure Levy, authorities would be able to use funds raised through the levy to secure affordable housing.

This could be secured through in-kind delivery on-site whereby the property would be sold to a registered provider at a discount from the market rate with the difference between the market rate and the discounted rate being offset against the cash liability.

To reduce risk to local planning authorities that the number of dwellings provided is less than currently delivered via S106 obligations, it is suggested that in the event of a fall in the housing market, that developers could be allowed to 'flip' the affordable housing to market housing to cover liability of levy.

Local authorities could also accept Infrastructure Levy payments in the form of land within or adjacent to a site. Through borrowing against further Infrastructure Levy receipts, other sources of funding, or in partnership with affordable housing providers, they could then build affordable homes, enabling delivery at pace.

An alternative option would be to allow a local authority or provider to purchase a proportion of properties on-site at a discounted price broadly equivalent to build costs. The proportion would be set nationally, and the developer would have discretion over which units were sold in this way.

24(a). Do you agree that we should aim to secure at least the same amount of affordable housing under the Infrastructure Levy, and as much on-site affordable provision, as at present? [Yes / No / Not sure. Please provide supporting statement.]

Yes.

Any changes to the existing model of delivery of affordable housing through planning gain must lead to no reduction in delivery and that can only be guaranteed by allowing the LPA to insist on delivery onsite as other options introduce uncertainty.

However, it is not clear how the proposed mechanism to ensure that delivery of affordable housing is maintained will actually be achieved. The suggested approach could result in less affordable housing.

The consultation states that "*This could be secured through in-kind delivery on-site, which could be made mandatory where an authority has a requirement, capability and wishes to do so*". It is not clear as to what this means. For example, who judges 'capability'? Is it something to be assessed through the Examination process? What happens in terms of the provision of affordable housing in those circumstances where an authority does not satisfy this statement?

One of the criticisms of the existing arrangements is the uncertainty of negotiation around affordable housing. Any replacement must introduce detailed mechanisms to address this. For example if "capability" as discussed above relates to the financial ability to make an acceptable capital contribution toward affordable

housing on the part of the receiving organisation, one way of creating this certainty would be to fix the valuation mechanism and level of contribution.

It is not clear as to how local authorities will have the means to specify the form and tenure of on-site provision. What factors will need to be taken in to account and how will viability issues be expected to be taken in to account? This should be based on the need at the point in time when a proposal is brought forward rather than being a one-time only need as need will change through time. However, it is recognised that there is a need to balance an ability to address emerging need/demand with a position of certainty to both the LPA and the applicant. For example, to enable a developer to properly account for the costs associated with providing the affordable housing onsite as early as possible.

24(b). Should affordable housing be secured as in-kind payment towards the Infrastructure Levy, or as a 'right to purchase' at discounted rates for local authorities? [Yes / No / Not sure. Please provide supporting statement.]

Yes

In-kind payment towards the Infrastructure Levy as this provides more flexibility as to who would then take ownership of properties.

In the event that it is decided to go down the 'right to purchase' route, there should be an opportunity for the local authority to put forward potential recipient landlords where they are not in a position to take on the stock themselves, and where the developer has identified a recipient has controls to ensure that the recipient is a suitable entity to own/manage affordable housing.

24(c). If an in-kind delivery approach is taken, should we mitigate against local authority overpayment risk? [Yes / No / Not sure. Please provide supporting statement.]

Yes, but only if there are adequate measures to ensure that the value of affordable housing is maintained in the event of a down turn in the housing market.

24(d). If an in-kind delivery approach is taken, are there additional steps that would need to be taken to support affordable housing quality? [Yes / No / Not sure. Please provide supporting statement.]

Yes, but the suggestion that local authorities should be able to take a cash option where no provider will take the affordable housing due to poor build quality is not considered to be appropriate as it will simply then result in local authorities having to commit resources to bring forward the affordable housing elsewhere.

5.1.5 Proposal 22: More freedom could be given to local authorities over how they spend the Infrastructure Levy (question 25)

Proposed to retain the provisions of the Community Infrastructure Levy whereby 25% of levy is spent in the area where development occurs, with money transferred to Parish Councils. Potential for greater flexibility for local authorities as to how the levy is spent, including improving services or reducing council tax. However, could also require ring-fencing to ensure that affordable housing provision remains at same as (or higher than) current levels.

25. Should local authorities have fewer restrictions over how they spend the Infrastructure Levy? [Yes / No / Not sure. Please provide supporting statement.]

Not sure

It is important that the impact of any particular development on a locality is

adequately offset by the provision of new or improved infrastructure. The suggestion that once core infrastructure has been addressed a local authority should have greater flexibility as to how monies are used, is supported but there will need to be a clear definition of what constitutes core infrastructure. It is important that no impression is created of planning permissions being bought and sold. This could be defined locally.

25(a). If yes, should an affordable housing 'ring-fence' be developed? [Yes / No / Not sure. Please provide supporting statement.]

Yes?

6.0 DELIVERING CHANGE

6.1 The White Paper recognise that there will be a need for transitional arrangements, from the current approach to that proposed in the White Paper. However, no detail is available at this time.

6.2 The government also recognise that the proposed changes will have significant resource implications for local authorities, in addition to current shortages. However, the consultation suggests that "*there must be a fundamental cultural change on how planning departments operate. They need to be more outward looking, proactively engaging with developers, businesses, architects and designers, as well as a wider cross-section of their local communities*".

6.3 It is recognised that other players, such as statutory consultees and the Planning Inspectorate will also need to transform to respond to the changes.

6.4.1 Proposal 23: As we develop our final proposals for this new planning system, we will develop a comprehensive resources and skills strategy for the planning sector to support the implementation of our reforms. In doing so, we propose this strategy will be developed including the following key elements (no questions)

The cost of the planning system should continue to be met by the main beneficiaries – landowners and developers. Fees for planning applications would continue to be set nationally and so would cover cost of processing planning applications.

The cost of preparing local plans and taking enforcement action is borne by local authorities. The consultation suggests that as part of new infrastructure levy that a proportion could be earmarked to cover other costs.

Reform should be accompanied by a significant enhancement in digital and geospatial capability and capacity across the planning sector to support high-quality new digital Local Plans and digitally enabled decision-making.

It is recognised different local planning authorities face different pressures and issues, and it will be important to develop a resourcing and skills framework which works for all authorities across the country. Government propose to work with local planning authorities, professional bodies and the wider planning sector to ensure views about implementation are considered.

6.4.2 Proposal 24: We will seek to strengthen enforcement powers and sanctions (no question)

It is proposed to review and strengthen the existing planning enforcement powers and sanctions available to local planning authorities to ensure they support the new planning system.

More powers to address intentional unauthorised development, consider higher fines, and look to ways of supporting more enforcement activity.

7.0 GENERAL OBSERVATIONS

7.1 Seeking improvements to the planning system is a laudable aim. However, a number of proposals seek to ensure speed which may be at odds with quality. Whatever decision is made by government needs to balance speed and efficiency with openness and transparency. Good decisions are good decisions however long they take. Bad decisions are something which the local community have to live with.

7.2 As already noted there is a lack of detail, which is to be expected from a White Paper, and no doubt through time the proposals will develop and evolve. However, a key aspect to a number of the proposals is that they would result in increased centralisation and the loss of local control. It is difficult to reconcile this with improving the planning system.

7.3 A key concern at this stage is the lack of any details regarding possible transition arrangements. The White Paper states that in terms of Local Plans "*The proposals allow 30 months for new Local Plans to be in place so a new planning framework, so we would expect new Local Plans to be in place by the end of the Parliament* ". The current Parliament is due to end in December 2024. There is a risk that the current review of the Local Plan could be impacted by these changes. However, there is insufficient certainty that the proposals as they are currently outlined will be implemented. It will be necessary to keep this matter under review and, if necessary, make adjustments to the scope and content of the review.

Policies and other considerations, as appropriate	
Council Priorities:	- Supporting Coalville to be a more vibrant, family-friendly town - Support for businesses and helping people into local jobs - Developing a clean and green district - Local people live in high quality, affordable homes - Our communities are safe, healthy and connected.
Policy Considerations:	The proposals outlined in the consultation have the potential to have a fundamental impact upon the Council's Local Plan, which is currently being reviewed.
Safeguarding:	None identified at this time.
Equalities/Diversity:	Some aspects of the proposals set out in the White Paper have a potential to have a negative impact upon some sectors of the community. For example, the greater use of digital technology could impact those without access to computers and so prohibit their participation in the planning system. Furthermore if proposals relating to affordable housing shift the role of specifying the affordable housing contribution in favour of the developer there is a risk that specialist provision will be reduced impacting on groups with protected characteristics.
Customer Impact:	No issues identified
Economic and Social Impact:	No specific issues identified, but see comments under policy considerations and risks.
Environment and Climate Change:	No specific issues identified, but see comments under policy considerations and risks.
Consultation/Community Engagement:	None
Risks:	The proposals set out in the White Paper would have significant resource implications for the Council.

	Depending upon the timing of any changes, there could be an impact upon the Local Plan review in terms of its scope, content and look. If transition arrangements are not put in place or are not robust, there is a risk that current work on the review could be jeopardised or lost. This matter will need to be kept under review.
Officer Contact	Ian Nelson Planning Policy Team Manager 01530 454677 ian.nelson@nwleicestershire.gov.uk

APPENDIX A

PILLAR ONE OVERVIEW

1. What three words do you associate most with the planning system in England?

2(a). Do you get involved with planning decisions in your local area? [Yes / No] 2(b). If no, why not? [Don't know how to / It takes too long / It's too complicated / I don't care / Other – please specify]

3. Our proposals will make it much easier to access plans and contribute your views to planning decisions. How would you like to find out about plans and planning proposals in the future? [Social media / Online news / Newspaper / By post / Other – please specify]

4. What are your top three priorities for planning in your local area? [Building homes for young people / building homes for the homeless / Protection of green spaces / The environment, biodiversity and action on climate change / Increasing the affordability of housing / The design of new homes and places / Supporting the high street / Supporting the local economy / More or better local infrastructure / Protection of existing heritage buildings or areas / Other – please specify]

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

CABINET – TUESDAY, 20 OCTOBER 2020

Title of Report	**LOCAL PLAN REVIEW – DRAFT OBJECTIVE 4 (SUSTAINABLE TRANSPORT)**	
Presented by	Councillor Robert Ashman Planning and Infrastructure Portfolio Holder	
Background Papers	National Planning Policy Framework Sustainability Appraisal Scoping Report 2020 Council Delivery Plan Leicester and Leicestershire Strategic Growth Plan	**Public Report:** Yes **Key Decision:** Yes
Financial Implications	The cost of the substantive Local Plan Review is met through existing budgets.	
	Signed off by the Section 151 Officer: Yes	
Legal Implications	The agreed draft objectives will be included in the next consultation stage for the Substantive Local Plan Review. This consultation must be undertaken in a way that accords with the council's agreed Statement of Community Involvement.	
	Signed off by the Monitoring Officer: Yes	
Staffing and Corporate Implications	No staffing implications associated with the specific content of this report. Links with the Council's Priorities are set out at the end of the report.	
	Signed off by the Head of Paid Service: Yes	
Purpose of Report	To reconsider the wording of the draft Local Plan Objective 4 which is concerned with sustainable transport for inclusion in the next stage of public consultation for the Substantive Local Plan Review.	
Reason for Decision	The preparation of the Local Plan is a Cabinet function.	
Recommendations	**THAT CABINET REQUEST THE LOCAL PLAN COMMITTEE NOTE THE REVISED WORDING OF DRAFT OBJECTIVE 4 AT PARAGRAPH 1.7 FOR INCLUSION IN THE NEXT PUBLIC CONSULTATION STAGE OF THE SUBSTANTIVE LOCAL PLAN REVIEW.**	

1. DRAFT OBJECTIVE 4

1.1 At its meeting on 14th July 2020, Cabinet considered a draft set of objectives for inclusion in the substantive Local Plan Review. Cabinet resolved to refer the objectives for consideration by the Local Plan Committee.

1.2 The Local Plan Committee met on 29th July 2020. Agreement was reached on 10 of the 11 objectives but Objective 4, which is concerned with sustainable transport, was not agreed. At the meeting, Councillor Legrys put forward specific revised wording for this objective.

1.3 The original wording for Objective 4 was as follows;

"4 - Reduce the need to travel and increase opportunities for cycling, walking and public transport use."

1.4 Councillor Legrys' proposed the following;

"4 - The Local Plan Review to plan for
- specific off-highway walking and cycling routes within NWL
- with particular consideration made to safeguard land for the provision of segregated off-highway walking/cycling routes to and from employment growth areas
- and an overall focus on the improvement of inter-community off-highway interconnectivity."

1.5 This amendment was not agreed and officers were asked to work with Councillor Legrys and Councillor Bridges (as chair of the Local Plan Committee) to find alternative wording. This would enable the themes from Councillor's Legrys' amendment to be reflected using wording which better matched the tone and overarching nature of the other 10 objectives.

1.6 The themes in the Councillor Legrys amendment can be summarised as

- Delivery of infrastructure
- Connectivity; and
- Safety

1.7 In respect of safety, this issue is already addressed in Objective 3 in the context of high quality development and does not to be further repeated in Objective 4. The following revised wording picks up the remaining two themes;

"4 - Reduce the need to travel and increase opportunities for cycling, walking and public transport use, including connecting homes, workplaces and facilities and through the delivery of dedicated new infrastructure.

1.8 Councillor Legrys has indicated to officers that he finds this proposed wording acceptable.

1.9 Cabinet is asked to give a positive recommendation to the Local Plan Committee to note this revised objective. Subject to Cabinet's and the Local Plan Committee's consideration, the 11 draft objectives will be part of the next public consultation for the substantive Local Plan Review.

Policies and other considerations, as appropriate	
Council Priorities:	The Council Priorities particularly relevant to the subject matter of this report are: - Our communities are safe, healthy and connected - Developing a clean and green district
Policy Considerations:	Adopted Local Plan National Planning Policy Framework
Safeguarding:	None specific
Equalities/Diversity:	The Local Plan Review as an entity will be subject to an Equalities Impact Assessment.
Customer Impact:	None specific
Economic and Social Impact:	The decision, of itself, will have no specific impact. The Local Plan Review as a whole will deliver positive economic and social impacts and these will be recorded through the Sustainability Appraisal.
Environment and Climate Change:	The decision, of itself, will have no specific impact. The Local Plan Review as a whole will deliver positive

	environmental and climate change benefits and these will be recorded through the Sustainability Appraisal.
Consultation/Community Engagement:	The draft objectives will be subject to public consultation as part of the plan preparation process. The consultation arrangements will be governed by requirements in the Statement of Community Involvement.
Risks:	A risk assessment for the Local Plan Review has been prepared and is kept up to date. As far as possible control measures have been put in place to minimise risks, including regular Project Board meetings where risk is reviewed.
Officer Contact	Ian Nelson - Planning Policy Team Manager 01530 454677 ian.nelson@nwleicestershire.gov.uk

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

CABINET – TUESDAY, 20 OCTOBER 2020

Title of Report	**FOOD SAFETY SERVICE DELIVERY PLAN 2020/21**	
Presented by	Councillor Andrew Woodman Community Services Portfolio Holder	
Background Papers	Food Standards Agency – Framework Agreement on Local Authority Food Law Enforcement. http://www.food.gov.uk/multimedia/pdfs/enforcement/frameworkagreementno5.pdf Food Standards Agency – Food Law Code of Practice (England) (Issue: March 2017) https://www.food.gov.uk/enforcement/enforcework/food-law	**Public Report:** Yes **Key Decision:** Yes
Financial Implications	The financial and staffing resources required are detailed in the Service Plan and are included in the approved budget for 2020/21	
	Signed off by the Section 151 Officer: Yes	
Legal Implications	All legal implications are detailed in the Service Plan	
	Signed off by the Monitoring Officer: Yes	
Staffing and Corporate Implications	There is a risk that additional resources may be required to deliver concurrent issues of the backlog of food hygiene inspections and covid-19 related activity.	
	Signed off by the Head of Paid Service: Yes	
Purpose of Report	To inform Members of the content of the Food Safety Service Delivery Plan 2020/21 as required by the Food Standards Agency To inform Members of the performance against the 2019/20 service delivery plan	
Reason for Decision	To approve the content of the Food Safety Service Delivery Plan 2020/21 as required by the Food Standards Agency.	
Recommendations	**(1) THAT THE ENVIRONMENTAL HEALTH FOOD SAFETY SERVICE DELIVERY PLAN 2020/21 APPENDED TO THIS REPORT BE APPROVED** **(2) THAT THE PERFORMANCE AND ACHIEVEMENTS IN 2019/20 BE NOTED**	

1.0 INTRODUCTION

1.1 The Food Safety function is delivered by the Environmental Health team. When providing the Food Safety function, the council must have regard to the 'Framework Agreement on Local Authority Food Law Enforcement' which sets out the standards agreed with the Food Standards Agency.

1.2 The Framework Agreement requires each food safety service to document and implement a Food Safety Service Delivery Plan in accordance with a specified standard. In addition a documented performance review of the plan is required to be carried out at least once a year. The framework agreement requires the Service Plan, together with the performance

review to be submitted for member approval to ensure local transparency and accountability.

1.3 The Environmental Health Food Safety Service Delivery Plan 2020/21 is attached at **Appendix 1.**

2.0 LINKS TO COUNCIL PRIORITIES AND OUTCOMES

2.1 The work of the food safety service links to two of the Council priorities, Business and Jobs and Homes & Communities.

Business and Jobs: The provision of regulatory advice and guidance provides a business with the confidence to grow. For example:

Regulatory advice can result in a business saving money by avoiding gold plated compliance;
By seeking advice from a regulator before opening or expanding, a business can avoid spending money in areas which fail to comply with the law;
Regulatory advice provides a business with reassurance and peace of mind;
Regulatory advice is free, avoiding a business the cost of appointing a private sector consultant;
Regulatory advice from a local government officer is viewed by business as 'straight from the horse's mouth', and can be relied upon.

Homes and Communities: The work of the service helps ensure our residents and visitors have safe and healthy places to work, eat and enjoy.

3.0 MAIN FOCUS OF THE 2020/21 PLAN

Pre covid-19 the plan was to focus work in the following areas:

- A programme of 558 food safety interventions consisting of inspection, auditing and sampling. Priority will be given to high risk establishments. (Paragraph 4.1.1 of Service Plan);

- A programme of food safety inspections/coaching visits targeting a selection of non-compliant food establishments (Paragraph 4.1.2 of Service Plan);

- An Earned Recognition approach for mobile food vendors that attend various events, markets and fairs across the Leicester and Leicestershire Enterprise Partnership (LLEP) area. Events in North West Leicestershire will include the Download music festival, Castle Donington and Timber, the National Forest Moira. Those mobile food vendors that **are** broadly compliant with hygiene law and have a Food Hygiene Risk Rating score of 3 or above will not receive any intervention unless an issue is identified, thereby recognising the hygiene standards achieved. This will reduce the regulatory burden on compliant business, a key objective of the Government. (Paragraph 4.1.3 of Service Plan);

- The provision of support to HMS Host Uk Limited under a Primary Authority Partnership (Paragraph 4.3);

- Investigation of food and food premises complaints (Paragraph 4.2), and all outbreaks and incidents of food related illnesses (Paragraph 4.6);

- The provision of information and advice on food safety to businesses and customers (Paragraph 4.4);

- A coordinated food, water and environmental sampling programme (Paragraph 4.5);

- The issuing of export certificates (Paragraph 4.8);

- To operate the inspection facility at East Midlands Airport (Paragraph 4.9). All products of animal origin and certain foods not of animal origin arriving at East Midlands Airport from a country outside the European Union will be inspected. Catch certificates for fish and fishery products entering the EU via East Midlands Airport will be issued;

- To support businesses demonstrating a potential to grow through joint visits with the Business Focus team;

- To promote the National Food Hygiene Rating Scheme for food establishments within the district. Food establishments will be encouraged to display their rating; (Paragraph 4.11)

4.0 IMPACT OF COVID-19 ON SERVICE PLAN

- The Environmental Health Officers and Food Safety Officer responsible for delivering the food safety service plan have been heavily involved in the response to covid-19.

- During the lockdown many of the businesses scheduled for inspections were forced to close. The focus of resource at this time was given to monitoring the business closures and responding to concerns raised by members of the public.

- The vast majority of the events scheduled have been cancelled which will impact on the advisory and sampling activity.

- Once the lockdown began to ease in June 2020 the team experienced a high demand from business owners requesting guidance on how to open safely. The food safety team provided support to businesses by guiding them to make their premises covid-secure.

- From July 2020 the Food Standards Agency directed local authorities to begin inspecting the highest risk businesses and those with a poor compliance history. This work did begin in July in North West Leicestershire.

- At the time of writing this report we are still awaiting direction from the Food Standards Agency to commence the programmed inspection of food establishments in the medium and low risk categories. Once this direction of given it is anticipated that there will be a backlog of approximately 400 interventions.

5.0 PERFORMANCE INDICATORS AND TARGETS

5.1 The food industry is regulated by a range of legislation that aims to keep our food safe. Our work with food businesses is focussed on helping them comply with food safety legislation and offering support and advice. This is seen as a critical area of our work by central government and the compliance levels of food establishments in our area are monitored and used as a measure of how our work impacts on business safety.

On 1 April there were 904 food businesses registered within our district, 727 of which are covered within the scope of the national food hygiene rating scheme. 707 of the 727 (97.2%) food businesses have a hygiene rating of 3, 4 or 5 (satisfactory standards or better). The profile of the food establishments by hygiene rating is as follows:

Food Hygiene Rating	Number of food establishments
0 – Urgent improvement necessary	0
1 – Major improvement necessary	9
2 – Improvement necessary	11
3 – Generally satisfactory	34
4 – Good	99
5 – Very Good	574

5.2 The following targets have been set:

Indicator	Annual Target 20/21
Number of food establishments improving hygiene standards by moving from 0, 1 or 2 (non-compliant) using the national food hygiene rating scheme to a 3,4 or 5	15
Percentage of programmed high risk (risk category A,B and non-compliant C) inspections achieved	100

6.0 SUCCESSES AND ACHIEVEMENTS IN 2019/20

6.1 Key successes in 2019/20 included:

- 97.2% of establishments that have received a hygiene rating have achieved a rating of 3 (Generally satisfactory) or higher (Good, Very Good); an increase of 0.8% from the previous year
- The number of establishments requiring improvement (rated 0,1,2) fell from 26 to 20 during 2019/20.
- The number of establishments demonstrating very good hygiene standards (rated 5) increased from 541 to 574 during 2019/20.

6.2 Business Compliance – Significant improvement

As a result of the work undertaken by the Service, standards of hygiene and safety at food establishments within North West Leicestershire have improved over recent years.

The table below shows how the percentage of food establishments rated as 3 or higher has increased from 89% to just over 97% over the past 8 years.

	April 2013	April 2014	April 2015	April 2016	April 2017	April 2018	April 2019	April 2020
Number of establishments within scheme	695	719	764	737	704	697	714	727
Number rated 3 or higher	620	663	718	712	674	675	688	707
Number rated 0, 1 and 2	75	56	46	25	30	22	26	20
Percentage rated 3 or higher	89%	92%	94%	96.6%	95.7%	96.8%	96.4%	97.2%
Percentage rated 0, 1 and 2	11%	8%	6%	3.4%	4.3%	3.2%	3.6%	2.8%

Policies and other considerations, as appropriate	
Council Priorities:	Insert relevant Council Priorities: - Support for businesses and helping people into local jobs - Our communities are safe, healthy and connected
Policy Considerations:	None noted
Safeguarding:	None noted
Equalities/Diversity:	Equality Impact Assessment already undertaken, issues identified actioned
Customer Impact:	Customers of food establishments (manufacturers, retailers, caterers and importers) can enjoy safe, hygiene food
Economic and Social Impact:	The work will enable the safe reopening of many businesses that were closed during the lockdown period. The work will help to build business and consumer confidence.
Environment and Climate Change:	None noted.
Consultation/Community Engagement:	Food Standards Agency Public Health England
Risks:	If the authority fails to discharge its duty imposed by the Food Safety Act 1990 the enforcement functions may be transferred to another authority. Adverse publicity, both locally and nationally may be received.
Officer Contact	Lee Mansfield Environmental Health Team Manager Lee.mansfield@nwleicestershire.gov.uk

This page is intentionally left blank

FOOD SAFETY

ENVIRONMENTAL HEALTH

SERVICE DELIVERY PLAN 2020-21

North West Leicestershire District Council

As Required By the Food Standards Agency

FOOD SAFETY
SERVICE DELIVERY PLAN 2020-2021

CONTENTS

FOOD SAFETY SERVICE DELIVERY PLAN 2020-2021

1. INTRODUCTION

This service plan has been produced in accordance with the Framework Agreement on Local Authority Official Feed and Food Controls.

This plan provides the basis on which the authority will be monitored and audited by the Food Standards Agency.

This plan should be read in conjunction with the Environmental Health Business Plan 2020/21.

2. AIM AND OBJECTIVES OF SERVICE

2.1 Aim

To protect public health in North West Leicestershire and ensure that the food imported, prepared, stored, sold and consumed in the district is safe to eat, through enforcement and education.

2.2 Objectives

- To undertake quality programmed interventions of food establishments (in land and point of entry) in line with their risk rating and intervention policy.
- To undertake an alternative enforcement strategy in low risk premises.
- To investigate all reports of food poisoning in line with service standards and take appropriate action.
- To investigate all service requests in line with service standards and inform complainants of outcomes and the reason for the outcomes.
- To undertake a programme of food sampling to demonstrate the importance of good hygiene and to check food safety systems are working.
- To further develop Primary Authority partnerships
- To maintain an accurate database.
- To undertake a programme of education aimed at the public and businesses.
- To undertake surveillance, inspection and sampling of imported foods.

2.3 Strategic Aims

The work of the food safety team makes an important contribution to the Council's priorities 'Business and Jobs' and 'Homes and Communities'.

2.4 Performance Indicators

Indicator	Annual Target 20/21
Number of food establishments improving hygiene standards by moving from 0, 1 or 2 (non-compliant) using the national food hygiene rating scheme to a 3,4 or 5	15
Number of support visits made to smaller food establishments and start-ups	200
Proportion of businesses that said they felt the requirements and feedback received by the inspector	85%

was reasonable	

2.5 **Service Standards**

All service users can expect and will receive an efficient and professional response.

Officers will identify themselves by name in all dealings with service users.

Officers will carry identification cards and authorisations at all time.

Service users will be informed of the name and telephone number of the officer who is responsible for their need.

All service requests will be responded to; however, anonymous requests may not be dealt with.

The following initial response times to service requests can be expected by service users:-

Immediate

Vermin in food premises.
Food poisoning outbreak.
Case of suspected food poisoning.
Mouldy food complaint.
Situations likely to result in an imminent risk to health.

Within 24 hours

Collection of a food complaint.
Inspection of imported food at East Midlands Airport
IUU – catch certificates

Within 3 days

Food Hygiene Rating Scheme – appeal application
Food Hygiene Rating Scheme – Re-score visit application
Food Hygiene Rating Scheme – Right to Reply request
Imported food enquiries – request for advice
All other food hygiene related complaints.

Within 5 days

Confirmed cases of all other food related illness or communicable disease.

Following a food hygiene intervention food business operators will receive a letter within 14 days. The letter will contain details of how to make representations to the Environmental Health Safety Team Leader or Environmental Health Team Manager.

All enforcement action will be taken in accordance with the Council's Enforcement Policy.

3. BACKGROUND

3.1 Profile of the Authority

North West Leicestershire District Council services an estimated population of 93,468 covering an area of 27,933 hectares. It is a predominately rural district with 2 main urban areas, Coalville and Ashby de la Zouch.

3.2 Organisational Structure

3.2.1 Democratic Structure

The Council is composed of 38 Councillors elected every four years. All Councillors meet together as the full Council. Meetings of the Council are normally open to the public. Councillors decide the Council's overall policies and set the budget each year. The Council will appoint a Leader, a Policy Development Group, regulatory bodies, an Audit and Governance Committee and other statutory, advisory and consultative bodies.

The Cabinet is responsible for most day-to-day decisions and comprises the Leader and his appointed Portfolio Holders. The Cabinet has to make decisions which are in line with the Council's budget and policy framework.

The Policy Development Group may make recommendations which advise the Cabinet and the Council on its policies, budget and service delivery as well as monitoring the decisions of the Cabinet.

3.2.2 Food Safety Team Structure

The Food Safety Team sits within the Environmental Health Safety Team which forms part of the Community Services Team. The team is managed by the Environmental Health Team Manager. In addition the following staff contribute to the food safety service:

Environmental Health Safety Team Leader
Environmental Health Officers (3 FTE)
Primary Authority Officer (1 Part time)
2 Food Safety Officers

The Environmental Health Team structure chart is attached at Appendix 2

In addition there is 1 Business Support Officer and 1 Business Support Assistant who support the work of the Food Safety Team.

The team submits any samples for microbiological analysis to the Public Health Laboratory Colindale, London and all other samples for analysis to the County Public Analyst (Wolverhamption Scientific Services and ALS).

Eville & Jones Ltd provide the Official Veterinary Surgeon at the border inspection post at East Midlands Airport. The Lead Official Veterinary Surgeon (OVS) is Patrik Vazan and Veterinary Manager is Rafael Pedregosa.

3.3 **Description and Scope of Service**

Proactive	**Reactive**
Programmed inspections Programmed surveillance visits Food sampling (including imported foods) Water sampling Primary Authority Partnerships Flight manifest checks (imported food) Advice / Coaching	Food hygiene complaints Food complaints Food poisoning investigations/outbreaks Food alerts / Incidents Advice / Coaching Food Import enquiries Catch certificates Export certificates New Business enquiries / Business Support Inspections of products of animal origin and high risk foods of non animal origin at the border inspection post/designated point of entry

3.4 **Demands on the Service**

The food safety service is based at the Council Offices situated in Coalville. The hours of opening are 8.45 – 5.00 Monday, Tuesday, Wednesday, Friday and 9.30am – 5.00 Thursday. Officers from the Food Team work outside normal office hours as the need arises.

The border inspection post situated at East Midlands Airport is manned on a reactive basis, as and when the service is required. The OVS is programmed to be sited at the inspection post 1 day a week.

3.4.1 There are 904 food establishments known to the team in the district. These comprise of:

41	Manufacturers
26	Distribution / Importer / Exporter
157	Retailers
680	Caterers

Of these there are 3 meat products and 1 dairy product manufacturers which have been approved as required by EC Regulation 853/2004.

3.4.2 East Midlands Airport is within the district. The border inspection post at East Midlands Airport (EMA) is managed by the Environmental Health Team. The officers of the food safety team are responsible for inspecting all fishery products from a third country entering the EU via the border inspection post at EMA. The OVS inspects all other products of animal origin entering the UK via the border inspection post. The officers of the food safety team are responsible for checking all 'high risk' foods not of animal origin from a third country entering the EU via the designated point of entry at EMA.

3.4.3 All food establishments are categorised according to their intervention frequency in accordance with the Statutory Food Law Code of Practice.

At 1 April 2020 the profile of premises within the district was:

Category	Number	Intervention Frequency
A (high risk)	1	At least every 6 months
B (high risk)	28	At least every 12 months
C (medium risk)	139	At least every 18 months
D (medium risk)	361	At least every 2 years
E (low risk)	327	A programme of alternative enforcement strategies at least every 3 years
Unrated	48	
Total registered food establishments	904	
Outside of programme (importers non-food)	13	Every 3 months (questionnaire)

Note: Category E premises must be subject to an alternative enforcement strategy or intervention, at least once during any three year period.

All transit sheds and importers not currently importing foodstuff will be contacted every 3 months.

The number of businesses owned by ethnic minorities whose first language is not English has no significant impact on the service.

3.5 **Enforcement Policy**

Officers within the Food Team take into account the principles of good enforcement set out in the Regulators' Code. The Council's general enforcement policy and specific food control enforcement policy incorporates the content of the Regulators' Code.

4. SERVICE DELIVERY 2020/2021

4.1 Food Establishment Interventions

4.1.1 Programmed Interventions

Council Policy: "that all food establishment interventions will be carried out in accordance with the Statutory Food Law Code of Practice and internal procedure: PN1.0 Food Interventions. Interventions will take place unannounced wherever possible."

The complete intervention programme for 2020/2021 is as follows:

Risk Category	Inspections due 2020/2021	Carried forward from 2019/20 programme	Total Programmed 2020/2021
A	2 (1 establishment)	0	2
B	24	5	29
C	100	5	105
D	181	14	195
E	103	24	127
Unrated	48	0	48
Importers (non food)	52	0	52

Total	510	48	**558**

Priority will be given to establishments within risk category A, B, unrated and non broadly compliant* C and D. It is estimated that 30% of establishments will receive one or more revisits. In addition to the above programme, all new food establishments will receive an initial inspection.

*NOTE: A 'broadly complaint' establishment is one that has an intervention rating score of not more than 10 points under each of the following parts of Annex 5, Part 2: level of (Current) Compliance, hygiene and level of (Current) Compliance – Structure and Part 3: Confidence in Management.

The Food Standards Agency has published the; 'E.Coli 0157 Control of Cross Contamination' guide providing critical information for food business operators and enforcement authorities. The guide aims to increase recognition of the threat of *E.coli* and identifies the need to have stringent measures in place to prevent transmission. It sets out controls in circumstances where food may be contaminated and is handled in the same establishment as ready-to-eat food. Given that very serious outbreaks and fatalities have been associated with this organism all food businesses will be made aware of the risks and will receive advice on the most effective ways of preventing infection.

Intervention Policy

Category	Planned Intervention
A (non compliant)	Full/Partial inspection/audit
B (non compliant)	Full/Partial inspection/audit
C (non compliant)	Full/Partial inspection/audit
D (non compliant)	Full/Partial inspection/audit monitoring / verification / official sampling or education/advice/ coaching
A (compliant)	Full/Partial inspection/audit
B (compliant)	Full/Partial inspection/audit
C (compliant)	Full/Partial inspection/audit Or Monitoring / verification / official sampling
D (compliant)	Full/Partial inspection/audit monitoring / verification / official sampling or education/advice/ coaching
E (compliant)	Self assessment questionnaire
Unrated	Full/Partial inspection/audit
Non food ETSF / Importers	Telephone questionnaire Liaison with UKBF

4.1.2 **High Risk Intervention Programme**

A selection of non compliant food establishments rated as either 0, 1 or 2 under the Food Hygiene Rating Scheme will be selected. Each establishment will receive interventions which may include full and partial inspections, coaching sessions, food safety management advice, mentoring from a compliant business and verification visits. Interventions will continue until such time that the Inspector considers the food establishment to be 'broadly complaint' with food hygiene law. At this point

interventions will cease. Each establishment will then receive their programmed full or partial inspection to determine if they have maintained their broadly compliant standard. Each establishment will be offered a chargeable re-rating inspection. Consideration will be given to the service of hygiene improvement notices where a business fails to secure improvements following structured, regular support and guidance.

The success of the project will be evaluated by the number of establishments that improving their food hygiene rating from 0,1 or 2 to at least a 3.

4.1.3 Better Business for All - Earned Recognition Scheme

The service will follow an earned recognition scheme when targeting resource to food hygiene controls large public gatherings such as the Download Music Festival. Those mobile food vendors that have a Food Hygiene Risk Rating score of 3 or above on the national food hygiene rating scheme will not receive an intervention unless the registering authority requests that an intervention is made. The objective of this approach is to reduce unnecessary regulatory burden on compliant businesses.

4.1.4 Inspection of aircraft

Aircraft are included within the definition of premises. The Food Law Code of Practice states that primary consideration should be given to the origin of the food on board, including water and other drinks, and the transport to, and loading of, the aircraft.
An audit of the sampling programme for the water on board aircraft will be undertaken.

4.1.5 Specialised Processes

The manufacture of meat and dairy products, in-flight catering, the inspection of third country imports of products of animal origin, the production of carbonated drinks and the production of crisps and snacks are all specialist areas of work undertaken within North West Leicestershire. The current post holders within the Food Safety Team hold adequate expertise within these specialist areas of work. When devising the departmental training needs, maintaining adequate knowledge in these areas of work is a priority.

Donington Park is situated within North West Leicestershire. A number of international sporting and musical events are held at the park. Officer time will be spent assisting with the planning of large events such as the Download music festival. This work will include the partial inspection of a proportion of food establishments trading at these events. Where water provision involves a temporary installation, work to ensure water safety will be undertaken.

A street trading consent scheme operates within North West Leicestershire. All mobile food establishments and static units trading within the District hold a ‘consent’ under the scheme.

4.2 Food Complaints

Council Policy: **“that all food complaints received are investigated in accordance with the Statutory Food Law Code of Practice and internal procedure note PN7.0: Food Complaints.”**

Based on previous years figures it is estimated that the team will receive in the range of 20 food complaints.

4.2.1 **Food Hygiene Service Requests**

Council Policy: **"that the Food Safety Team undertake unprogrammed visits as a result of a complaint about the standards of hygiene at a food establishment, a new establishment opening, new management taking over or due to a request by another agency"** e.g. Defra, Ofsted.

This will include most service requests received by the food team regarding standards of hygiene e.g. including complaints about:-

- cleanliness in premises
- drainage defects
- pest problems
- service requests for inspections by other statutory bodies, e.g. Ofsted, Animal Health
- service requests for guidance from new owners of food establishments

These interventions do not form part of the programmed interventions.

Based on previous years figures it is estimated that the number of service requests received relating to standards of hygiene will be approximately 30.

4.3 **Primary Authority**

Council Policy: **"to have regard to the Primary Authority Scheme".**

Council Policy: **"to have regard to the information (national inspection plans and approved assured advice) provided on the Primary Authority website before undertaking an intervention at an establishment with a Primary Authority."**

The Council has a Primary Authority partnership with HMS Host Uk Limited.

Based on previous years figures it is estimated that the team will receive in the range of 5 - 10 originating authority complaints from other local authorities.

4.4 **Support and Advice to Business (including import enquiries)**

Council Policy: **"to provide advice to both established and new food establishments".**

The Leicester and Leicestershire Regulatory Services Partnership and Better Business for All (BBfA) Steering Group was established in 2011. The overriding objective of the Partnership and the BBfA programme is to improve engagement with local businesses and provide them with advice and guidance to assist in reducing the burden of regulation on business.

In 2020/21 the following food safety support is available to businesses:

Inspection – An officer will provide advice to every business during a routine food hygiene inspection.

Coaching - If requested by a Food Business Operator a one to one coaching session will be undertaken to assist them in complying with the law.

High Risk Establishment Enhanced Support Project – A selection of non compliant businesses will receive an enhanced level of support to assist them in becoming compliant. It is hoped that by increasing the level of support and advice to non compliant businesses, the number of businesses 'broadly compliant' with food hygiene legislation will increase. The additional support will only be available to those businesses which demonstrate a willingness to improve and maintain hygiene standards.

Food safety advice is available on the Council's website. Advice is also available on the food standards agency website.

Any business requesting advice and guidance in other areas of regulation or non regulatory support will be signposted to the LLEP Business Gateway advice line or website.

4.5 Sampling Programme

4.5.1 Food Sampling

Council Policy: **"to take part in National and Local Food Sampling Programme."** The food items which form part of this programme are selected by the Leicester and Leicestershire Food Best Practice Group based on known or potential problem areas. All samples are taken in accordance with the Statutory Food Law Code of Practice. The programme is detailed at Appendix 1.

In addition to the sampling programme food samples may be submitted for examination as part of a programmed intervention, complaint, infectious disease investigation or imported food surveillance.

Using sampling as an Official Control intervention is highlighted in the Statutory Food Law Code of Practice. Some samples may be sent to the Public Analyst for analysis. The authority is charged for this service.

The number of samples that can be submitted for examination free of charge is allocated by the Public Health Laboratory Service (PHLS).

4.5.2 Water Sampling (Commercial Premises & Aircraft)

Council Policy: **"that routine sampling of mains water is not undertaken."**

However, sampling of mains water may take place as a result of a complaint or concern.

Council Policy: "to audit the sampling and monitoring programme in place to ensure the quality of water on-board aircraft at East Midlands Airport.

4.5.3 Private Water Supplies

The district has the following private water supplies and distribution systems in its area:

	Large	Small	Single domestic

Private Water Supplies	4	2	11
Distribution Systems	2		

The Authority has a statutory duty to risk assess private water supplies within its district and then conduct a sampling program based upon the risk assessment.

Sampling Programme 2020/21
The 4 large supplies will be sampled twice during the year
2 small supplies will be sampled every 5 years. None of the small supplies will be sampled during 2020/21
Single domestic supplies will not routinely be sampled but sampling can be carried out on request
Private Distribution Systems will be sampled based on the outcome of the risk assessment

4.6 **Infectious Disease Control**

Council Policy: **"to investigate all food borne diseases."**

The team receives notifications from Public Health England relating to residents/visitors within the district suffering from a notifiable infectious disease. The team may also receive informal notifications of suspected food poisoning from members of the public. Non food related infectious diseases are investigated based on advice from the Consultant for Communicable Disease Control (CCDC).

Based on previous year's figures it is estimated that the team will receive in the range of 110-120 formal or informal notifications of food related infectious diseases.

4.7 **National Food Safety Incidents**

Council Policy: **"to deal with food alerts in accordance with the Statutory Food Law Code of Practice.**

The Food Standards Agency issues a 'Product Withdrawal Information Notice' or a 'Product Recall Information Notice' to let local authorities and consumers know about problems associated with food. In some cases, a 'Food Alert for Action' is issued. This provides local authorities with details of specific action to be taken.

The team receives food alerts via EHC net messaging system and the FSA Enforcement mailbox. Food Alerts: Alerts 'For Action' are referred for the urgent attention of the Environmental Health Team Manager or Environmental Health Safety Team Leader.

Based on previous year's figures the section is likely to receive less than 10 alerts for action.

4.8 **Food Export Health Certificates**

Health certificates are issued to food businesses who wish to export foodstuff outside the EU. They are provided to help local exporters meet the food safety requirements. The team check that the business is registered with us and that we are satisfied with the food hygiene standards before issuing the certificate.

Based on previous year's figures the team is likely to issue approximately 100 export certificates.

Any free trade agreement with the EU may have an impact on demand for export health certificates.

4.9 Imported Foods at Point of entry

4.9.1 Border Control Post (BCP) – Products of animal origin

The service manages and operates the border control post at East Midlands Airport (EMA). The BCP is subject to audits and verification visits by Animal Health, an Agency of Defra. These currently take place twice a year.

All products of animal origin arriving at EMA from a country outside the EU have to be inspected at the border inspection post. Officers from the Food Safety Team have responsibility for inspecting all fishery products and an Official Veterinary Surgeon (OVS) has been appointed by the authority to inspect all other products of animal origin.

Any free trade agreement with the EU may have an impact on demand for the inspection of products of animal origin.

4.9.2 Catch certificates (Fish and Fishery Products)

On 1st January 2010 an EU regulation came into force to combat illegal, unreported and unregulated fisheries. The regulation requires a catch certificate for all imports and landings of fish and fish products into the EU by third countries. The service issue catch certificates for fish and fishery products entering the EU via East Midlands Airport.

Based on previous year's figures the team is likely to issue approximately 250 catch (exemption) certificates.

Any free trade agreement with the EU may have an impact on demand for catch certificates.

4.9.3 Border Control Post (BCP) – High risk foods not of animal origin

In 2014 the Food Standards Agency granted a DPE/DPI status to East Midlands airport for all ambient stable products listed within Commission Regulation (EU) No 996/2012, No 91/2013 and No 1152/2009. Officers of the food safety team will respond to all foodstuffs pre-notified.

Based on previous year's figures the team is likely to process less than 10 consignments.

Any free trade agreement with the EU may have an impact on demand for inspection of high risk foods of non-animal origin.

4.9.4 Surveillance

A risk based programme of surveillance will be carried out. This will involve officers carrying out checks of flight manifests and visits to transit sheds. Sampling of foodstuffs found may be undertaken.

Each of the importers / ETSF and transit shed operators that do not currently handle foodstuffs will be contacted every 3 months.

Due to the flight schedule the monitoring of 'live' manifests has to be undertaken outside normal office hours. In addition some manifests checked will not be 'live'. They will be viewed after the freight has left the airport. The checking of such manifests provides a useful auditing tool.

4.9.5 **Sampling**

A sampling programme will be carried out, being informed by the national monitoring plan and local intelligence and information.

4.9.6 **Liaison/Management of Port Health**

In 2008 a multi-agency East Midlands Airport Port Health Group was established. Membership of this group includes Public Health England, North West Leicestershire DC, Leicestershire and Rutland Primary Care Trust, East Midlands Airport and UK Border Force.

Council Policy: **"To contribute to the delivery of the multi-agency Port Health Group at East Midlands Airport."**

A representative from the Environmental Health will attend meetings of this group.

Regular communication with Border Force is in place.

4.10 **Other non-official control interventions**

Council Policy: **"to raise the awareness of the public to the potential causes of food poisoning."** Throughout the year articles will be published in the local press and on the Council web pages regarding food safety matters.

<u>Food Poisoning in the Home</u>
Once again we will be communicating the key messages as suggested by the Food Standards Agency during national food safety week.

<u>Effective hand washing</u>
To raise the awareness of the importance of hand washing in preventing the spread of disease such as covid-19 the hand washing machine with ultra violet light will be offered to workplaces, schools and child nurseries around the district.

4.11 **Food Hygiene Rating Scheme**

North West Leicestershire District Council operates the national Food Hygiene Rating Scheme (FHRS). The scheme provides consumers with information regarding the hygiene standards identified in food establishments at the time of the last intervention.

The data is managed by the Environmental Health Safety Team Leader on an ongoing basis and a data upload carried out a minimum of every 13 days.

The profile of the scheme will be maintained through the issue of press releases and social media messages with compliance standards at businesses being recognised by issuing certificates/stickers.

4.12 Licensing/Consents

The team is consulted prior to the issue of premises licences (new and variations) under the Licensing Act 2003. All take-away premises and food mobiles trading between 11.00 p.m. and 5.00 a.m. require licensing under the Act. The Safety Team will respond to any new applications and variation applications received and make representations if there are public safety or public nuisance concerns.

Officer time will be spent assisting with the planning of large events such as the Download Music Festival, Outbreak Festival and the World Superbikes motor racing event.

The team is consulted prior to the issue of new consents and existing non compliant traders under the Street Trading Scheme. All mobile food establishments and static units trading within the District hold a 'consent' under the scheme.

4.13 Liaison with Other Organisations and Internal Communication

A member of the Environmental Health Service is represented on the following groups/meetings:

External/Multi-agency Groups:

- Leicestershire and Rutland CIEH Food Best Practice Group
- Association of Port Health Authorities Liaison Groups (Border Inspection Post, Airports, Environmental Health & Hygiene)
- East Midlands Airport multi-agency Port Health Group
- Leicestershire CIEH Environmental Health Managers Group
- Public Health England Liaison Group
- Idox Uniform User Group
- Download event planning meetings
- Donington Park event planning meetings
- Cattows Farm event planning meetings
- Better Business for All Partnership – Task & Finish Groups
- UK Border Force liaison meetings
- East Midlands airport – Cargo Development

Internal Groups:

- Safety Team Meeting
- Monthly 121's/Performance meetings
- NWLDC Idox user group

5. RESOURCES

5.1 Financial Allocation

The budget for the provision of the food safety service is £315,480. The general expenses incurred by the service such as training, salaries and administrative costs are budgeted for as part of the budget for Environmental Health.

5.2 Staffing Allocation

It is the Council's policy to authorise officers appropriately in accordance with their qualifications and experience having regard to the Statutory Food Law Code of Practice. All officers have been authorised in accordance with the internal procedure PN 5.0: Authorisation of Officers.

The nominated lead officer for food safety is the Environmental Health Safety Team Leader.

5.2.1 The details of the staffing levels in the section are as follows:

Environmental Health Team Manager – The post holder is an Environmental Health Officer with responsibility for the food hygiene, health and safety, Port Health, Pest Control, Animal Welfare and licensing functions of the Council. The post holder is authorised under the Food Safety and Hygiene England) Regulations 2013. Food related work = 0.4 FTE (Non operational)

Environmental Health Team Leader – The post holder supervises the operational work of the Team, and undertakes food safety work. The post holder is fully authorised under the Food Safety and Hygiene England Regulations 2013. Food related work = 0.7 FTE (Imported foods= 0.05FTE)

Environmental Health Officer – The post holder undertakes food safety work and also carries out duties under the Health and Safety at Work etc. Act 1974. The post holder is fully authorised under the Food Safety and Hygiene England Regulations 2013. Food related work = 0.7 FTE (Imported foods= 0.05FTE)

Environmental Health Officer – The post holder undertakes food safety work and also carries out duties under the Health and Safety at Work etc. Act 1974. The postholder's food safety enforcement powers are restricted by authorisation to non official controls only. Food related work = 0.7 FTE (Imported foods= 0.05FTE)

Environmental Health Officer (Part time) – The post holder undertakes food safety work and also carries out duties under the Health and Safety at Work etc. Act 1974. The post holder is fully authorised under the Food Safety and Hygiene England Regulations 2013. Food related work = 0.3 FTE (Imported foods= 0.05FTE)

Environmental Health Officer (Part time – 18.125 hours) – The post is currently vacant with the work being carried out by an inspector employed on a temporary basis through an agency. The post holder is fully authorised under the Food Safety and Hygiene England Regulations 2013. Food related work = 0.4 FTE (Imported foods= 0.05FTE)

Primary Authority Officer (Part time – 18.125 hours) The post is currently vacant with the work being carried out by an inspector employed on a temporary basis through an agency. The post holder undertakes the Primary Authority role, working with HMS Host Uk Limited

Food Safety Officer – The post holder undertakes food safety work and also carries out limited duties supporting an appointed inspector under the Health and Safety at Work etc. Act 1974. The postholder's food safety enforcement powers are restricted by authorisation. Food related work = 0.9 FTE (Imported foods= 0.05FTE)

Food Safety Officer – The post is currently vacant.

There is 1 Business Support Officer and 1 Business Support Assistant providing support to the food safety section. Food related work = 0.1 FTE and 0.1 FTE

5.3 **Staff Development/Training**

The Environmental Health Team has embraced the principles of the Best Employee Experience (B.E.E) Project. The individual Performance and Development Reflection meetings are a key element of North West Leicestershire District Council`s aim to support its employees by providing them with the development and learning required. Additional training requirements will be identified during the appraisal process and will form a training plan for the team. Officers from the team will be given training which will take into account any changes in legislation or guidance as and when required.

NOTE: Each Food Officer is required by the Statutory Food Law Code of Practice to do a minimum of 10 hours core training.

6. QUALITY ASSESSMENT / INTERNAL MONITORING

6.1 A performance management system is in place within the Environmental Health Team in order to assess the quality of the service provided and the performance against agreed standards and how this information is communicated.

The system involves:

- The Environmental Health Team Manager (EHTM) and Environmental Health Team Leader (EHTL) monitoring the team performance against the SDP on a monthly basis.

- 1 Accompanied inspection and 1 Reality check will be carried out for each Authorised Officer each year by the Environmental Health Team Leader.

- Additional detailed checks to assess the adequacy of the post inspection paperwork will be carried out by the EHTL on a monthly basis and the check will be on a minimum of two inspections each month.

- Every year the EHTM will check 1 inspection carried out by the EHTL.

- All statutory notices will be checked by the EHTL or in their absence the EHTM before service.

- The EHTL will check the notice log on a monthly basis to ensure all outstanding notices have been checked off.

- Monitoring of service requests will be carried out by EHTL. A minimum of 1 service request will be checked every month.

- The EHTM will receive all completed customer satisfaction forms and will reply to any questionnaires requesting a response. Any adverse comments will be reacted to appropriately.

- The EHTM will receive a review of the questionnaires each quarter.

- The EHTL will check the sampling log every quarter to ensure its completeness and accuracy and to ensure that appropriate follow action has been taken.

When undertaking the above checks will be made to ensure the Code of Practice and internal procedures are being complied with.

Internal procedures have been and will continue to be developed in consultation with the Leicester & Leicestershire Food Best Practice Group to ensure consistency across the County.

7. COMMUNICATION

7.1 Communication within the Team

7.1.1 Every month the EHTM meets with the Head of Community Services.

7.1.2 Every month the EHTM meets with the EHTL to discuss any issues and the previous month's performance. In addition on-going issues are discussed as and when they arise.

7.1.3 Each month the EHTL meets with the officers individually to discuss performance.

7.1.4 Each month officers are given a summary of their previous month's performance.

7.1.5 At least every quarter there is a team meeting where specific issues are discussed with the Food Team.

8. REVIEW 2019/2020

8.1 Review against the Service Plan

The figures detailed below relate to data retrieved from the premises database on April 1st 2020.

8.1.1 Programmed Inspections (Inland)

The number of premises and their risk ratings is changeable throughout the year. The number of inspections not carried out by the end of March 2020 is used to determine the percentage of those inspections completed.

93% of the planned inspection programme was achieved – (Risk categories A, B, C, D and unrated)

100% of highest risk interventions were achieved (Category A)

Risk Category	Total inspections programmed 2019/2020	Inspections remaining due at end of year	% of due inspections achieved
A	10 (5 establishments)	0	100
B	36	4	89
C	95	4	96
D	144	14	90
E	102	24	77
Unrated	37	0	100

Importers (non food)	52	0	100
Total	476	46	**90**

8.1.2 **Support Programme – Business Growth**

A programme of support was delivered to 20 food establishments all of which were identified as potential for business growth. Face to face visits were made by the Environmental Health team and referrals made to our Business Focus (Economic Development) teams where further business support was provided.

8.1.3 **Food Hygiene Service Requests**

	2016/17	2017/18	2018/19	2019/20
Food Hygiene Service Requests including drainage	19	13	61	73
Regarding problems with pests and rubbish	3	3	4	4
Total	22	16	65	77

8.1.4 **Food Complaints**

	2016/17	2017/18	2018/19	2019/20
Foreign bodies in food	4	2	13	8
Mouldy foods	1	3	2	0
Chemical issues	1	0	1	1
Labelling of food	1	0	2	2
Allergy related	NA	NA	NA	4
Total	7	5	18	15

8.1.5 **Home Authority Principle**

	2016/17	2017/18	2018/19	2019/20
Food Complaints – Home / Originating Authority	1	0	0	0

8.1.6 **Advice to Businesses**

The Safety Team and Customer Contact Centre gave advice over the telephone to customers. Detailed figures for this work are not recorded.

	2016/17	2017/18	2018/19	2019/20
Requests for food safety advice	12	19	45	49

8.1.7 **Sampling**

	2016/17	2017/18	2018/19	2019/20
Food Samples - Total	43	1	10	17
Food Samples - unsatisfactory (number)	17	0	1	3
Environmental Samples - Total	8	34	9	5
Environmental Samples - unsatisfactory (number)	4	10	7	3
Private Water Supply Samples -	21	17	25	7

Total				
Private Water Supply Samples - % unsatisfactory	28% (6)	35% (6)	60% (15)	43% (3)
Large Public Event Samples - Total	42	0	13	27
Large Public Event - % unsatisfactory	2% (1)	0	0	0

8.1.8 **Infectious Disease**

	2016/17	2017/18	2018/19	2019/20
Reported suspected food poisoning cases	15	4	37	49
Infectious Disease notifications	117	115	69	NA
Most common disease and number	Campylo bacter - 79	Campylo bacter - 83	Campylo bacter - 36	NA

8.1.9 **Responding to National & Serious Localised Food Safety Incidents**

If there is a problem with a food product that means it should not be sold, then it might be 'recalled' (when the product is taken off the shelves or customers are asked to return the product). If the problem presents a serious risk to public health the Food Standards Agency issues a 'Food Alert For Action' requiring all local authorities to take direct action. The Environmental Health – Food Safety Team responds to all alerts for action.

8.1.10 **Border Control Post (POAO)**

Year	Enquiries received	Catch (exemption) Certificates Issued	Total consignments CVED	Fish (EHO)	Other products (OVS)	Total Rejected	% Rejected
2005/06	N/A	N/A	86	28	58	18	21
2006/07	107	N/A	149	76	73	21	14
2007/08	112	N/A	129	41	88	53	41
2008/09	147	N/A	172	31	141	107	62
2009/10	126	N/A	161	20	141	83	52
2010/11	184	255	154	13	141	62	40
2011/12	113	246	84	15	69	33	39
2012/13	65	251	67	6	61	22	33
2013/14	41	258	68	8	60	9	13
2014/15	55	256	71	16	55	6	9
2015/16	40	249	52	8	44	6	11
2016/17	28	254	52	1	51	7	13
2017/18	23	255	68	11	57	28	41
2018/19	61	251	33	3	30	12	40
2019/20	89	242	41	5	36	27	66

8.1.11 **Imported High Risk Foods of Non- Animal Origin**

In 2014 the Food Standards Agency granted DPE/DPI status to East Midlands for a for all ambient stable products listed within Commission Regulation (EU) No 996/2012, No 91/2013 and No 1152/2009.

In 2014 an EHO visited those businesses thought to be handling imported foodstuffs. An inspection was carried out and a risk rating of the premises undertaken. These premises have since formed part of the inspection programme.

Each of the 13 importers that has confirmed they do not currently handle foodstuffs were contacted every 3 months for surveillance purposes. Any premises identified as handling imported foodstuffs will receive an inspection.

Programmed Quarterly Checks of Non food importers

Number of premises	Number of quarterly checks programmed	Number of checks carried out	% of planned checks carried out
13	52	52	100%

Designated Point of Entry / Designated Point of Inspection

	Number of consignments presented	Product description	Number cleared
2016/17	3	Pistachio nuts	3
2017/18	23	Tea – China (21), dried grapes – Turkey (2)	23
2018/19	7	Tea - China	7
2019/20	1	Tea – China	1

8.1.12 **Surveillance of flight manifests**

A risk based programme of surveillance was carried out in 2019/20 to identify any foodstuffs subject to import controls. 21 flight manifests were checked, focussing on flights direct from or transiting through 3rd Countries. Two carriers and flights were targeted.

Although commercial food consignments were identified on manifests, none of the foodstuffs were subject to import controls. Although no foodstuffs requiring inspection were found the surveillance did provide a knowledge of the flight routes and the nature and volumes of consignments imported.

8.1.13 **Food Export Health Certificates**

	Number of export certificates issued	Number of customers
2016/17	98	1
2017/18	210	4
2018/19	122	5
2019/20	37	4

8.1.14 **Liaison with Other Organisations**

During 2019/20 the following liaison took place:-

Leicestershire & Rutland CIEH Food Best Practice Group / Technical Sub-Committee: Quarterly meetings. The Environmental Health Team Leader attended the quarterly meetings

East Midlands Airport Multi-agency Port health Meeting: This group did not meet.

Leicestershire CIEH Environmental Health Managers Group: The Environmental Health Team Manager attended the quarterly meetings.

Leicestershire Better Business for All Steering Group / Partnership: The Environmental Health Team Manager attended the quarterly meetings.

Health Protection Agency Liaison Group: The Environmental Health Team Leader attended all of the scheduled meetings.

East Midlands Airport – EU Exit Border Planning Group – The Environmental Health Team Manager attended the meetings.

8.1.15 **Education & Awareness Initiatives** (**Other Non-Official Controls Interventions)**

Low risk food establishments – Risk Category E

Food establishments that are considered to be low risk to consumers are categorised as risk category E. Low risk establishments do not form a part of the inspection programme. However a programme of alternative enforcement strategies must be in place with each establishment receiving an intervention at least once during any three year period.

Each of the 102 establishments categorised as low risk and due an intervention were contacted and/or visited to assess their compliance with food hygiene law. Standards were satisfactorily assessed at 78 of the 102 establishments. Work will continue at the remaining 24 establishments during 2020.

Food Safety Week

Food Safety Week took place in June and focussed on raising awareness and understanding of the work Environmental Health teams do across England, Wales and Northern Ireland.

The council took part in a national campaign led by the Food Standards Agency. We used social media to raise awareness of the national food hygiene rating scheme and to tell the story of the work carried out to ensure consumers in NWL remain safe.

National Food Hygiene Rating Scheme

The food hygiene rating scheme was promoted using press releases and social media (Twitter).

8.2 **Staffing Allocation**

1 full-time and 1 part-time EHO post was vacant for a proportion of the year. Temporary resource was appointed through a recruitment agency.

8.3 **Food Hygiene training Undertaken by Staff**

Food safety update
FSA consistency exercise
Food detention and seizure
Border Inspection Post / Port Health procedures
Pubic Health England Symposium
Private Water Supplies
Severn Trent Water health liaison
Listeria
Food Poisoning Outbreaks
Shelf Life Testing
STEC and E.coli Workshop
IUU Regulations
Vacuum Packing and Sous Vide – Module 1,2,3

8.4 **Enforcement Actions Taken**

Hygiene Improvement Notices were served	13
Prohibition related notices	0
Seizure of food notices	0
Detention / Remedial Action Notices	0
Enforcement Notices (Regulation 20) under The Trade and Related Animal Product Regulations – Fail Veterinary checks at BIP	27
Enforcement Notices (Regulation 32(6)) under The Trade and Related Animal Product Regulations – Introduced in breach of regulations	0
Regulation 32 Notices under Official Feed and Food Controls (England) Regulations	0
Cautions for offences under food hygiene legislation	0
Conviction for offences under food hygiene legislation	0
Prohibition of Person from managing a food business	0

8.5 **Performance Outcomes**

As a result of the work undertaken by the service, standards of hygiene and safety at many food establishments within North West Leicestershire improved.

A programme of support was delivered to over 400 food establishments. All relevant food establishments have been rated using the National Food Hygiene Rating Scheme.

The number of establishments requiring improvement (rated 0,1 and 2) decreased from 26 to 20 during 2019/20.

The percentage of establishments demonstrating broad compliance with food hygiene law increased from 96.4% to 97.2% during 2019/20.

Performance Targets:

Indicator	Target	Actual
Number of growth businesses in receipt of face to face support from Environmental Health and referred to Business Focus	20	20
Number of food establishments moving from a position of	15	30

non compliance (rated 0, 1 or 2) to broadly compliant (rated 3, 4 or 5) using the national food hygiene rating scheme		

8.6 **Issues for 2020/21**

- Building on the successes of the previous programmes, to undertake an enhanced support programme targeting a number of the non compliant food establishments
- To provide co-ordinated support with the Business Focus team targeting food establishments showing the potential to grow
- To further develop the Primary Authority role with HMS Host
- To introduce and promote the digital food registration process developed by the Food Standards Agency

9. **IMPACT OF COVID-19**

- The covid-19 pandemic has accelerated the introduction of agile working using Microsoft surface pro devices.
- The pandemic resulted in many businesses having to close for a significant period of time. Environmental Health Officers have been used to monitor compliance with the business closure regulations.
- As businesses began to re-open many required advice and support on what they could do to comply with covid-19 government guidance such as social distancing measures. EHOs have provided businesses with this support.
- The government ceased the programmed inspection of businesses from mid March. The focus of the work between March and July was reactive, responding to concerns reported to us, monitoring compliance with business restriction regulations and remotely monitoring standards at those businesses previously non compliant with food hygiene law.
- From mid July the government permitted the programmed inspection of non compliant food establishments.

Insert once finalised

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

CABINET – TUESDAY, 20 OCTOBER 2020

Title of Report	**REVIEW OF CORPORATE GOVERNANCE POLICIES**	
Presented by	Councillor Nicholas Rushton Corporate Portfolio Holder	
Background Papers	UK Anti-corruption strategy 2017-2022 Bribery Act 2010 Data Protection Act 2018 Money Laundering and Terrorist Financing (Amendment) Regulations 2019 Investigatory Powers Act 2016 Home Office Codes of Practice 2018	**Public Report:** Yes **Key Decision:** Yes
Financial Implications	The update of policies will protect the Councils finances	
	Signed off by the Section 151 Officer: Yes	
Legal Implications	The update of policies will ensure compliance with current legislation	
	Signed off by the Monitoring Officer: Yes	
Staffing and Corporate Implications	Any staffing or corporate implications are detailed in the policies.	
	Signed off by the Head of Paid Service: Yes	
Purpose of Report	To provide Cabinet's comments on the Councils Revised Governance Policies	
Reason for Decision	To ensure that the council has an up to date suite of governance policies in place reflecting the law and best practice	
Recommendations	**THAT CABINET:** **1. NOTE THE COMMENTS FROM THE AUDIT AND GOVERNANCE COMMITTEE ITS MEETING ON THE 22 JULY 2020** **2. APPROVE THE CORPORATE GOVERNANCE POLICES LISTED IN PARAGRAPH 2**	

1.0 BACKGROUND

1.1 The Council is responsible for ensuring that its business is conducted in accordance with the law and appropriate standards. In discharging this responsibility the Council has in place arrangements for governance of its affairs and staff.

1.2 The following documents constitute the Council's suite of Corporate policies:

Policy	Last reviewed

Anti-Fraud and Corruption Policy	2015
Anti-Money Laundering Policy	2015
RIPA Policy	2016
Information Management	Not been to members
Data Protection Policy	Not been to members
Confidential Reporting (Whistleblowing) Policy	2016
ICT & Cyber Security Policy	2019
Risk Management Strategy	2018
Local Code of Corporate Governance	2017

2.0 POLICY REVIEWS

The policies have been reviewed by a team comprising Legal, Internal Audit, ICT, the Monitoring Officer, the Strategic Director of Housing and Customer Services, the Data Protection Officer and the Section 151 Officer.

The main changes to each policy are summarised below:

2.1 Anti-Fraud and Corruption Policy

An internal audit in 2016/2017 recommended that a review of the Council's fraud policy framework be undertaken to confirm the Council's Policies were up to date. In 2018 Leicester City Council undertook the review on behalf of the District Council concluding that the Anti-Fraud and Corruption and Anti-Money Laundering policies should be updated.
The following changes to the Anti-Fraud and Corruption Policy have been made:

- A clarification of the definitions of Corruption and Bribery to reflect those in the HM Government – UK Anti-corruption strategy 2017-22 and the Bribery Act 2010.
- The reinforcement of the culture of the Council's opposition to Fraud and Corruption
- Setting out the commitment to take action against those who offend against the Council
- Setting out the commitment to take disciplinary action where there is a breach of the policy
- An update to the details of external auditors, to reflect the new 5 year contract
- A clarification of the role and responsibility of CLT
- Outlining how the policy complies with new Data Protection legislation, the Data Protection Act 2018

2.2 Anti-Money Laundering Policy

The following changes to the Anti-money Laundering Policy have been made:

- An update to the Councils commitment to reflect the new legislation, Money Laundering and Terrorist Financing (Amendment) Regulations 2019

- An update to the definition of Money Laundering to give a more detailed definition within the policy
- An update to the details of the Money Laundering Reporting Officer (MLRO) and deputy MLRO as new appointments have been made since the last policy

2.3 Confidential Reporting (Whistleblowing Policy)

The following changes to the Confidential Reporting (Whistleblowing) Policy have been made:

- A clarification of the application of legislation to reflect the changes that it has to be in the public interest and only covers workers.
- The refinement of the Policy aims to be specific as to who the policy covers
- An update to the contact details of the officer to whom concerns should be raised due to structural changes
- An update to reference the new Data Protection legislation, the Data Protection Act 2018

2.4 Risk Management Policy

The following changes to the Risk Management Policy have been made:

- The adoption of a regular review of the Risk Management Strategy every two years.
- A move to a more specific, mitigation based and regular review approach.
- Audit and Governance Committee to receive regular updates of the Risk Register and mitigation plans.
- A clarification on some reporting issues in terms of when and what groups and meetings are involved.
- The provision of additional clarity regarding the role of particular staff roles and responsibilities.
- An update to reflect current practice in terms of timing and process.
- Editorial 'tidying up' and updating.
- A commitment to continue to review the corporate risks quarterly and recommend any changes through CLT prior to the information being presented to this Committee and onwards to Cabinet.

2.5 RIPA Policy

In June 2020 a virtual inspection by the Investigatory Powers Commissioner's Office was undertaken and further to this the following changes have been made to the Corporate Policy and Procedure on the Regulation of Investigatory Powers Act 2000 (RIPA) Policy:

- An amendment of the policy name to include reference to new legislation, the Investigatory Powers Act 2016 (IPA);
- The addition of reference to the IPA, what it authorises and how to obtain an authorisation. The IPA governs the acquisition of communications data, for example the address to which a letter is sent, the time and duration of a phone call, the telephone number or e-mail address of the originator and recipient, and the location of the device from which a communication was made;
- The addition of reference to the most up to date codes of practice from the Home Office;
- The addition of reference to changes in how children (under 18s) can be used as informants (known as Covert Human Intelligence Sources);
- The addition of reference to the use of the Council owed drone:
    - Consideration should be given to whether or not the drone will capture personal information;
    - If personal information is likely to be captured:

        - persons should be notified in advance (so it does not constitute covert surveillance); and
        - consider how to minimise this intrusion into people's privacy;
    - The inclusion of a warning to staff not to use personal devices (e.g. mobile phones or computers) to carry out investigations for work purposes (e.g. accessing a person of interest's social media account from a personal device);
    - An update to include reference to data retention periods to ensure any information obtained is deleted in accordance with the Council's Information Management Policy.

2.6 Information Management Policy

The following changes to the Information Management Policy have been made:

- A style change – update of the logo used
- An update to Information Management Team Structure and reference to corporate Information Champions
- The inclusion of reference to the Privacy and Electronic Communications Regulations (PECR) – This relates to the way data is used for marketing and is not limited to that which identifies personal data. Whilst the PCER have been in place since 2003, on the 25th May 2018 it became a requirement to comply with both PECR and GDPR. There is some overlap between the two but the overall aim is to protect data and complying with PECR helps comply with GDPR and vice versa.

As a result of the changes to working arrangements arising from COVID 19, the Council is working with other Leicestershire authorities to create a shared approach to dealing with homeworking within the policy. This will be brought forward at a later date.

2.7 Data Protection Policy

The Data Protection policy remains largely up to date as it was reviewed in 2019. The only amendments that have been made are to update the policy owner and reviewers.

These updates reflect the ownership of the policy and ensure that monitoring is objective.

2.8 ICT & Cyber Security Policy

The following changes to the ICT and Cyber Security Policy have been made:

- Spelling and grammar
- An update to some homeworking guidelines
- The inclusion of IT assets and how they are managed, as this was missing previously
- The addition of information relating to Cyber security including the process and procedure to report a cyber-incident
- An update to the use of 2 factor authentication and use of the Swivel mobile App
- The addition of l information about virtual meetings and the privacy of those meetings

2.9 Local Code of Corporate Governance

The Local Code of Corporate Governance continues to reflect the Council's current corporate governance arrangements and therefore only presentational and contextual changes have been made.

The Code was last reviewed and updated in 2017 in line with joint guidance on

corporate governance by the Chartered Institute of Public Finance & Accountancy (CIPFA) and the Society of Local Authority Chief Executives (SOLACE).

3.0 COMMENTS FROM AUDIT AND GOVERNANCE COMMITTEE

This Report along with the appended policies were taken to the Audit and Governance Committee on the 22 July 2020. The minutes of this committee are appended to this report at appendix 10.

In summary the Audit and Governance Committee did not propose any amendments to the policies themselves but they requested that members be told of the changes made and how they impact on them. In response, a members bulletin article is being drafted by officers which will be published once Cabinet has approved the updated policies.

Policies and other considerations, as appropriate	
Council Priorities:	- Supporting Coalville to be a more vibrant, family-friendly town - Support for businesses and helping people into local jobs - Developing a clean and green district - Local people live in high quality, affordable homes - Our communities are safe, healthy and connected
Policy Considerations:	Not applicable
Safeguarding:	Not applicable
Equalities/Diversity:	Where personal and sensitive data is held to ensure equal opportunities, this is done in a secure and compliant manner.
Customer Impact:	Ensuring transparency of policies for accountability that the all services and contact with customers is done so in line with up to date and relevant policies.
Economic and Social Impact:	Not applicable
Environment and Climate Change:	Not applicable
Consultation/Community Engagement:	All policies have been considered by the Audit and Governance Committee.
Risks:	As part of its Corporate Governance arrangements, the Council must ensure that Risk management is considered and satisfactorily covered in any report put before elected Members for a decision or action.
Officer Contact	Elizabeth Warhurst Head of Legal and Commercial Services elizabeth.warhurst@nwleicestershire.gov.uk

This page is intentionally left blank

APPENDIX 1

ANTI-FRAUD AND CORRUPTION POLICY

A guide to the Council's approach to preventing fraud and corruption and managing suspected cases.

Version Control

Version No	Author	Date
2.1	Anna Wright Senior Auditor	September 2015
2.2	Lisa Marron Audit Manager	October 2019

Contents

Anti-Fraud and Corruption Policy

1. Introduction

1.1 North West Leicestershire District Council has a duty to ensure that it safeguards the public money that it is responsible for. The Council expects the highest standards of conduct and integrity from all that have dealings with it including staff, members, contractors, volunteers and the public. It is committed to the elimination of fraud and corruption and to ensuring that all activities are conducted ethically, honestly and to the highest standard of openness and accountability so as to protect public safety and public money.

1.2 All suspicions or concerns of fraudulent or corrupt practise will be investigated. There will be no distinction made in investigation and action between cases that generate financial benefits and those that do not. Any investigations will not compromise the Council's commitment to Equal Opportunities or the requirements of the Human Rights Act or any other relevant statutory provision.

2. Scope

2.1 This policy provides an overview of the measures designed to combat any attempted fraudulent or corrupt act, whether attempted internally or externally. The policy is designed to:

- Encourage prevention;
- Promote detection;
- Ensure effective investigation where suspected fraud or corruption has occurred;
- Prosecute offenders where appropriate ; and
- Recover losses in all instances of fraud or financial irregularity where possible.

3. Definitions

3.1 Fraud

3.1.1 The Fraud Act 2006 is legislation that has been introduced in order to provide absolute clarity on the subject of fraud. Section 1 of the Act introduced a new general offence of fraud and three ways of committing it:

- Fraud by false representation
- Fraud by failing to disclose information; and
- Fraud by abuse of position.

3.1.2 Fraud by false representation requires:

- Dishonesty;
- An intent to make gain or cause loss; and
- The person makes the representation knowing that it is or might be untrue or misleading.

3.1.3 Fraud by failing to disclose information requires:

- Dishonesty;
- An intent to make gain or cause loss; and
- Failure to disclose information where there is a legal duty to disclose.

3.1.4 Fraud by abuse of position requires:

- Dishonesty;
- An intent to make gain or cause loss; and
- Abuse of a position where one is expected to safeguard another person's financial interests.

3.2 Corruption

3.2.1 Corruption is a form of dishonesty or criminal activity undertaken by a person or organisation entrusted with a position of authority, often to acquire illicit benefit.

3.3 Bribery

3.3.1 Broadly the Bribery Act 2010 defines bribery as giving or receiving a financial or other advantage in connection with the "improper performance" of a position of trust, or a function that is expected to be performed impartially or in good faith.

3.4 Money Laundering

3.4.1 Money laundering describes offences involving the integration of the proceeds of crime, or terrorist funds, into the mainstream economy. Whilst the risk of money laundering to the Council is relatively low and the provision of The Money Laundering Regulations 2007 do not strictly apply to the Council, the Council has adopted an Anti-Money Laundering policy as good practice. This policy supports staff in complying with the money laundering provisions included within the Proceeds of Crime Act 2002 and the Terrorism Act 2000.

4. Culture

4.1 We have determined that the culture and tone of the organisation will be one of honesty and opposition to fraud and corruption. We will not tolerate malpractice or wrongdoing in the provision of our services and are prepared to take vigorous action to stamp out any instances of this kind of activity. The fight against fraud and corruption can only be truly effective where these acts are seen as anti-social unacceptable behaviour and whistle blowing is perceived as a public-spirited action.

4.2 The prevention/detection of fraud/corruption and the protection of public money are responsibilities of everyone, both internal and external to the organisation. The Council's elected members and employees play an important role in creating and maintaining this culture. They are positively encouraged to raise concerns regarding fraud and corruption, immaterial of seniority, rank or status, in the knowledge that such concerns will wherever possible be treated in confidence. The public also has a role to play in this process and should inform the Council if they feel that fraud/corruption may have occurred. The Nolan Committee on Standards in Public Life set out the seven guiding principles (Appendix A) that apply to people who serve the public.

4.3 Concerns must be raised when members, employees or the public reasonably believe that one or more of the following has occurred or is in the process of occurring or is likely to occur:

- A criminal offence;
- A failure to comply with a statutory or legal obligation;
- Improper or unauthorised use of public or other official funds;
- A miscarriage of justice;
- Maladministration, misconduct or malpractice;

- Endangering an individual's health and/or safety;
- Damage to the environment; and
- Deliberate concealment of any of the above.

4.4 The Council will ensure that any allegations received in any way, including by anonymous letter or telephone call, will be taken seriously and investigated in an appropriate manner. The Council has a Confidential Report (Whistleblowing) policy that sets out the approach to these types of allegation in more detail.

4.5 The Council will take action against those who defraud the Council or who are corrupt or where there has been financial malpractice. There is, of course, a need to ensure that any investigation process is not misused and, therefore, any abuse (such as employees raising malicious allegations) may be dealt with as a disciplinary matter.

4.6 Where fraud or corruption has occurred due to a breakdown in the Council's systems or procedures, the Head of Service will ensure that appropriate improvements in systems of control are implemented in order to prevent re-occurrence.

5. Responsibilities

5.1 Responsibilities of Elected Members

5.1.1 As elected representatives, all members of the Council have a duty to protect the Council and public money from any acts of fraud and corruption. This is done through existing practice, compliance with the Members' Code of Conduct, the Council's Constitution including Financial Regulations and Standing Orders and relevant legislation.

5.2 Responsibilities of the Monitoring Officer

5.2.1 The Monitoring Officer is responsible for ensuring that all decisions made by the Council are within the law. The Monitoring Officer's key role is to promote and maintain high standards of conduct throughout the Council by developing, enforcing and reporting appropriate governance arrangements including codes of conduct and other standards policies.

5.3 Responsibilities of the Section 151 Officer

5.3.1 The Head of Finance has been designated as the statutory officer responsible for financial matters as defined by s151 of the Local Government Act 1972. The legislation requires that every local authority in England and Wales should 'make arrangements for the proper administration of their financial affairs and shall secure that one of their officers has the responsibility for the administration of those affairs'.

5.3.2 Under the Head of Finance's responsibilities, 'proper administration' encompasses all aspects of local authority financial management including;

- Compliance with the statutory requirements for accounting and internal audit;
- Managing the financial affairs of the Council;
- The proper exercise of a wide range of delegated powers both formal and informal;
- The recognition of the fiduciary responsibility owed to local tax payers.

Under these statutory responsibilities the Section 151 Officer contributes to the anti-fraud and corruption framework of the Council.

5.4 Responsibilities of Employees

5.4.1 Each employee is governed in their work by the Council's Standing Orders and Financial Regulations, and other codes on conduct and policies (Employee Code of Conduct, Health and Safety Policy, IT Strategy, IT Security Policy). Included in the Employee Code of Conduct are guidelines on Gifts and Hospitality, and advice on professional and personal conduct and conflicts of interest. These are issued to all employees when they join the Council. Appropriate disciplinary procedures will be invoked where there is a breach of policy.

5.4.2 Employees are responsible for ensuring that they follow instructions given to them by management, particularly in relation to the safekeeping of the assets of the Council.

5.4.3 Employees are expected always to be aware of the possibility that fraud, corruption and theft may exist in the workplace and be able to share their concerns with management.

5.5 Role of the Leicestershire Revenues and Benefits Partnership Fraud Investigation Team

5.5.1 The Fraud Team based at the Leicestershire Revenues and Benefits Partnership are responsible for the investigation of all revenues and benefit related alleged/suspected fraud cases. Due to the specialised nature of these investigations, a separate sanctions policy has been developed that covers all aspects of the investigation process.

5.6 Role of the External Auditors

5.6.1 Independent external audit is an essential safeguard of the stewardship of public money. This is currently carried out by Mazars through specific reviews that are designed to test (amongst other things) the adequacy of the Council's financial systems and arrangements for preventing and detecting fraud and corruption. It is not the external auditor's function to prevent fraud and irregularities, but the integrity of public funds is at all times a matter of general concern. External auditors are always alert to the possibility of fraud and irregularity, and will act without undue delay if grounds for suspicion come to their notice.

5.7 Role of the Public

5.7.1 This policy, although primarily aimed at those within or associated with the Council, enables concerns raised by the public to be investigated, as appropriate, by the relevant person in a proper manner.

5.8 Conflicts of Interest

5.8.1 Both elected members and employees must ensure that they avoid situations where there is a potential for a conflict of interest. Such situations can arise with externalisation of services, internal tendering, planning and land issues etc. Effective role separation will ensure decisions made are seen to be based on impartial advice and avoid questions about improper disclosure of confidential information.

6. Prevention and Deterrence

6.1 Responsibilities of the Senior Management Team

6.1.1 Managers at all levels are responsible for the communication and implementation of this policy. They are also responsible for ensuring that their employees are aware of the Council's policies and procedures relating to financial management and conduct and that the requirements are being met. Managers are expected to create an environment in which their staff feel able to approach them with any concerns they may have about suspected irregularities. Special arrangements may be applied from time to time for example where employees are responsible for cash handling or are in charge of financial systems and systems that generate payments, for example payroll or the Council Tax system. These procedures should be supported by relevant training.

6.1.2 Management has responsibility for the prevention of fraud and corruption within all departments. It is essential that managers understand the importance of soundly-designed systems which meet key control objectives and minimise opportunities for fraud and corruption. They are responsible for assessing the potential for fraud and corruption within their own department's activities and for implementing appropriate strategies to minimise this risk.

6.1.3 The Council recognises that a key preventative measure in dealing with fraud and corruption is for managers to take effective steps at recruitment stage to establish, as far as possible, the honesty and integrity of potential employees, whether for permanent, temporary or casual posts and agency staff. The Council's formal recruitment procedures contain appropriate safeguards in the form of written references, the verification of qualifications held and employment history. Disclosure and Barring Service (DBS) checks are undertaken for employees working with or who may have contact with children and vulnerable adults.

6.2 Role of Internal Audit

6.2.1 Internal Audit plays a preventative role in trying to ensure that systems and procedures are in place to prevent and deter fraud and corruption. Internal Audit may be requested to investigate cases of suspected financial irregularity, fraud or corruption, except Benefit fraud investigations and Single Person Discount fraud, in accordance with agreed procedures. Within the Financial Procedures Rules in the Constitution, representatives of Internal Audit have the authority to:

- enter any council owned or occupied premises or land at all times (subject to any legal restrictions outside the council's control);
- have access at all times to the council's records, documents and correspondence;
- require and receive such explanations from any employee or member of the council as he or she deem necessary concerning any matter under examination; and
- require any employee or member of the Council to produce cash, stores or any other Council owned property under their control.

Internal Audit liaises with management to recommend changes in procedures to reduce risks and prevent losses to the Authority.

6.3 Working with others and sharing information

6.3.1 The Council is committed to working and co-operating with other organisations to prevent fraud and corruption and protect public funds. The Council may use personal information and data-matching techniques to detect and prevent fraud, and ensure public money is targeted and spent in the most appropriate and cost-effective way. In order to achieve this,

information may be shared with other bodies for auditing or administering public funds including the Cabinet Office, the Department of Work and Pensions, other local authorities, National Anti-Fraud Network, HM Revenues and Customs, and the Police.

6.4 National Fraud Initiative (NFI)

6.4.1 The Council participates in the National Fraud Initiative (NFI). This requires public bodies to submit a number of data sets, for example payroll, council tax, and accounts payable (but not limited to these) which is then matched to data held by other public bodies. Any positive matches (e.g. an employee on the payroll in receipt of housing benefit) are investigated.

6.5 Data sharing

6.5.1 In the interests of protecting the public purse and the prevention and detection of fraud, members of staff are actively encouraged to report any instances of fraud. We have published fair processing notices on our website and also display this information in our public areas, notifying members of the public that we will share information held between departments and other 3rd party organisations as appropriate in order to prevent and detect crime.

6.6 Training and awareness

6.6.1 The successful prevention of fraud is dependent on risk awareness, the effectiveness of training and the responsiveness of staff throughout the Council. The Council recognises that the continuing success of this policy and its general credibility will depend in part on the effectiveness of training and awareness for members and employees and will therefore take appropriate action to raise awareness levels.

6.7 Disciplinary Action

6.7.1 The Council's Disciplinary Procedures will be used to facilitate a thorough investigation of any allegations of improper behaviour by employees. Theft, fraud and corruption are serious offences which may constitute gross misconduct against the Council and employees will face disciplinary action if there is evidence that they have been involved in these activities, including benefit fraud. Disciplinary action will be taken in addition to, or instead of, criminal proceedings depending on the circumstances of each individual case.

6.7.2 Members will face appropriate action under this policy if they are found to have been involved in theft, fraud or corruption against the Authority. Action will be taken in addition to, or instead of criminal proceedings, depending on the circumstances of each individual case but in a consistent manner. If the matter is a breach of the Members Code of Conduct then it will be dealt with under the arrangements agreed by the Council in accordance with the Localism Act 2011.

6.8 Prosecution

6.8.1 In terms of proceedings the Council will endeavour to take action in relevant cases to deter others from committing offences against the Authority. Any prosecution will be in accordance with the principles contained within The Code for Crown Prosecutors.

6.9 Publicity

6.9.1 The Council will optimise the publicity opportunities associated with anti-fraud and

corruption activity within the Council. Wherever possible, where the Council has suffered a financial loss action will be taken to pursue the recovery of the loss.

6.9.2 All anti-fraud and corruption activities, including the update of this policy, will be publicised in order to make employees and the public aware of the Council's commitment to taking action on fraud and corruption when it occurs.

7. Detection and Investigation

7.1 Although audits may detect fraud and corruption as a result of the work that they are undertaking, the responsibility of the detection of financial irregularities primary rests with management. Included within the audit plans are reviews of system controls including financial controls and specific fraud and corruption tests, spot checks and unannounced visits.

7.2 In addition to Internal Audit, there are numerous systems and management controls in place to deter fraud and corruption but it is often the vigilance of employees and members of the public that aids detection. In some cases frauds are discovered by chance or 'tip-off' and the council will ensure that such information is properly dealt with within its Confidential Reporting (Whistleblowing) policy.

7.3 The Council is committed to the investigation of all instances of actual, attempted and suspected fraud committed by employees, Members, consultants, suppliers and other third parties and the recovery of funds and assets lost through fraud.

7.4 Any suspected fraud, corruption or other irregularity should be reported to Internal Audit. The Audit Manager will decide on the appropriate course of action to ensure that any investigation is carried out in accordance with Council policies and procedures, key investigation legislation and best practice. This will ensure that investigations do not jeopardise any potential disciplinary action or criminal sanctions.

7.5 Action could include:

- Investigation carried out by Internal Audit staff;
- Joint investigation with Internal Audit and relevant directorate management;
- Directorate staff carry out investigation and Internal Audit provide advice and guidance;
- Referral to the Police.

7.6 The responsibility for investigating potential fraud, corruption and other financial irregularities within the Council lies mainly (although not exclusively) with the Internal Audit section.

8. Raising Concerns

8.1 All suspected or apparent fraud or financial irregularities must be raised, in the first instance, directly with the manager or if necessary in accordance with the Council's Confidential Reporting (Whistleblowing) Policy. Advice and guidance on how to pursue matters of concern may be obtained from the Council's nominated contact points who are:

- Chief Executive: bev.smith@nwleicestershire.gov.uk
  Telephone 01530 454500
- Monitoring Officer: elizabeth.warhurst@nwleicestershire.gov.uk

Telephone 01530 454762

- Section 151 Officer: tracy.bingham@nwleicestershire.gov.uk
  Telephone 01530 454707
- Audit Manager: lisa.marron@nwleicestershire.gov.uk
  01530 454728

Appendix A

The Seven Principles of Public Life

Selflessness

Holders of public office should take decisions solely in terms of the public interest. They should not do so in order to gain financial or other material benefits for themselves, their family, or their friends.

Integrity

Holders of public office should not place themselves under any financial or other obligation to outside individuals or organisation that might influence them in the performance of their official duties.

Objectivity

In carrying out public business, including making public appointments, awarding contracts or recommending individuals for rewards and benefits, holders of public office should make choices on merit.

Accountability

Holders of public office are accountable for their decisions and actions to the public and must submit themselves to whatever scrutiny is appropriate to their office.

Openness

Holders of public office should be as open as possible about all the decisions and action that they take. They should give reasons for their decisions and restrict information only when the wider public interest clearly demands.

Honesty

Holders of public office have a duty to declare any private interests relating to their public duties and to take steps to resolve any conflicts arising in a way that protects the public interest.

Leadership

Holders of public office should promote and support these principles by leadership and example.

Committee on Standards in Public Life – The Nolan Report (1995)

This page is intentionally left blank

ANTI MONEY LAUNDERING POLICY

A guide to the Council's anti-money laundering safeguards and reporting arrangements.

May 2020

Contents

Anti-Money Laundering Policy

1. Introduction

1.1 The Council is committed to the highest possible standards of conduct and has, therefore, put in place appropriate and proportionate anti-money laundering safeguards and reporting arrangements. Although local authorities are not directly covered by the requirements of the Money Laundering and Terrorist Financing (Amendment) Regulations 2019, they are bound by the Proceeds of Crime Act 2002 and the Terrorism Act 2006, both of which place a number of duties and responsibilities on local authorities and employees and member of the same, in order that they do not find themselves subject to criminal prosecution.

2. Scope of the Policy

2.1 This policy applies to all employees, whether permanent or temporary, and Members of the Council. Its aim is to enable employees and Members to respond to a concern they have in the course of their dealings for the Council. Individuals who may have a concern relating to a matter outside work should contact the Police.

3. Definition of Money Laundering

3.1 Money laundering is a term designed to cover a number of offences. These offences relate to the improper handling of funds that are the proceeds of criminal acts, or terrorist acts, so that they appear to come from a legitimate source. It relates to both the activities of organised crime but also to those who benefit financially from dishonest activities such as receiving stolen goods. The Proceeds of Crime act 2002 (POCA), as amended by the Serious Organised Crime and Police Act 2005, creates a range of criminal offences arising from dealing with proceeds of crime.

The four main offences that may be committed under money laundering legislation are:

- Concealing, disguising, converting, transferring or removing criminal property from anywhere within the UK;
- Entering into or becoming concerned in an arrangement which a person knows or suspects facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person;
- Acquiring, using or possessing criminal property*;
- Entering onto or being concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property ** by concealment, removal, transfer or in any other way:

It is also an offence to attempt, conspire or incite to commit any of the above offences and to aid, abet, counsel or procure the commission of any of the above offences.
*Criminal property is something which constitutes a person's benefit from criminal conduct or represents such benefit; it is not limited to money and there is no minimum amount.

**Terrorist Property includes money or other property likely to be used for terrorism, proceeds of terrorist acts, and proceeds of acts carried out for the purposes of terrorism.
There are also two 'third party' offences:

- Failing to disclose information relating to money laundering offences (in respect of both criminal property and terrorist property) where there is reasonable grounds for knowledge or suspicion *** ; and,
- Tipping off or informing someone who is, or is suspected of being involved in money laundering activities, in such a way as to reduce the likelihood of or

prejudice an investigation.

*** It is important to note that whilst the disclosure obligations and tipping off offences in relation to criminal property will not always strictly apply to local authorities all individuals and business' have an obligation to report knowledge, reasonable grounds for belief or suspicion about the proceeds from terrorism, proceeds of acts carried out for the purposes of terrorism or fiancé likely to be used for terrorism, where that information has come to them in the course of their business or employment.

3.2 The Terrorism Act made it an offence of money laundering to become concerned in an arrangement relating to the retention or control of property likely to be used for the purpose of terrorism, or resulting from acts of terrorism.

3.3 Although the term 'money laundering' is generally used to describe the activities of organised crime for most people it will involve a suspicion that someone they know, or know of, is benefiting financially from dishonest activities.

3.4 Potentially very heavy penalties (unlimited fines and imprisonment up to fourteen years) can be handed down to those who are convicted of one of the offences above.

4. Requirements of the Money Laundering Legislation

4.1 The main requirements of the legislation are:

- To appoint a money laundering reporting officer;
- Maintain client identification procedures in certain circumstances;
- Implement a procedure to enable the reporting of suspicions of money laundering;
- Maintain record keeping procedures.

5. The Money Laundering Reporting Officer (MLRO)

5.1 The Council has designated the Section 151 Officer as the Money Laundering Reporting Officer (MLRO). She can be contacted on 01530 454707 or at tracy.bingham@nwleicestershire.gov.uk.

In the absence of the MLRO or instances where it is suspected that the MLRO themselves are involved in suspicious transactions, concerns should be raised with the Deputy Section 151 Officer. She can be contacted on 01530 454492 or at anna.wright@nwleicestershire.gov.uk.

6. Client Identification Procedures

6.1 Although not a legal requirement, the Council has developed formal client identification procedures which must be followed when Council land or property is being sold. These procedures require individuals and, if appropriate, companies to provide proof of identity and current address.

If satisfactory evidence is not obtained at the outset of a matter, then the transaction must not be progressed and a disclosure report, available on iNet, must be submitted to the Money Laundering Reporting Officer.

All personal data collected must be kept in compliance with the Data Protection Act 2018.

7. Reporting procedure for Suspicions of Money Laundering

7.1 Where you know or suspect that money laundering activity is taking/has taken place, or become concerned that your involvement in a matter may amount to a prohibited act under the Act, you must disclose this as soon as practicable to the MLRO. The disclosure should be within 'hours' of the information coming to your attention, not weeks or months.

7.2 Your disclosure should be made to the MLRO using the disclosure form, available on iNet. The report must include as much detail as possible including:

- Full details of the person involved;
- Full details of the nature of their/your involvement;
- The types of money laundering activity involved;
- The dates of such activities;
- Whether the transactions have happened, are ongoing or are imminent;
- Where they took place;
- How they are undertaken;
- The (likely) amount of money/assets involved; and
- Why, exactly, you are suspicious.

Along with any other available information to enable the MLRO to make a sound judgement as to whether there are reasonable grounds for knowledge or suspicion of money laundering and to enable her to prepare her report to the National Crime Agency (NCA), where appropriate. You should also enclose copies of any relevant supporting documentation.

7.3 If you are concerned that your involvement in the transaction would amount to a prohibited act under sections 327-329 of the Proceeds of Crime Act 2002, then your report must include all relevant details, as you will need consent from the NCA, via the MLRO, to take any further part in the transaction – this is the case even if the client gives instructions for the matter to proceed before such consent is given. You should therefore make it clear in the report if such consent is required and clarify whether there are any deadlines for giving such consent e.g. a completion date or court deadline.

7.4 Once you have reported the matter to the MLRO you must follow any directions she may give you. You must NOT make any further enquiries into the matter yourself, any necessary investigation will be undertaken by the NCA. Simply report your suspicions to the MLRO who will refer the matter on to the NCA if appropriate. All members of staff will be required to co-operate with the MLRO and the authorities during any subsequent money laundering investigation.

7.5 Similarly, at no time and under no circumstances should you voice any suspicions to the person(s) whom you suspect of money laundering, even if the NCA has given consent to a particular transaction proceeding, without the specific consent of the MLRO; otherwise you may commit a criminal offence of 'tipping off'.

7.6 Do not, therefore, make any reference on a client file, to a report having been made to the MLRO – should the client exercise their right to see the file, then such a note will obviously tip them off to the report having been made and may render you liable to prosecution. The MLRO will keep the appropriate records in a confidential manner.

8. Consideration of the disclosure by the Money Laundering Reporting Officer

8.1 Upon receipt of a disclosure report, the MLRO must note the date of receipt on his section of the report and acknowledge receipt of it. She should also advise you of the timescale within which he expects to respond to you.

8.2 The MLRO will consider the report and any other available internal information he thinks relevant e.g.

reviewing other transaction patterns and volumes;
the length of any business relationship involved;
the number of any one-off transactions and linked one-off transactions;
any identification evidence held.

and undertake such other reasonable inquiries she thinks appropriate in order to ensure that all available information is taken into account in deciding whether a report to the NCA is required (such enquiries being made in such a way as to avoid any appearance of tipping of those involved). The MLRO may also need to discuss the report with you.

8.3 Once the MLRO has evaluated the disclosure report and any other relevant information, she must make a timely determination as to whether;

there is an actual or suspected money laundering taking place; or

whether there are reasonable grounds to know or suspect that this is the case; and

whether she needs to seek consent from the NCA for a particular transaction to proceed.

8.4 Where the MLRO does so conclude, then she must disclose the matter as soon as practicable to the NCA on their standard report form and in the prescribed manner, unless he has a reasonable excuse of non-disclosure to the NCA (for example, if you a lawyer and you wish to claim legal professional privilege for not disclosing the information).

8.5 Where the MLRO suspects money laundering but has a reasonable excuse for nondisclosure, then she must note the report accordingly, she can then immediately give her consent for any ongoing or imminent transactions to proceed. In cases where legal professional privilege may apply, the MLRO must liaise with the Council's Monitoring Officer to decide whether there is a reasonable excuse for not reporting the matter to the NCA.

8.6 Where consent is required from the NCA for a transaction to proceed, then the transaction(s) in question, must not be undertaken or completed until the NCA has given specific consent, or there is deemed consent through the expiration of the relevant time limits in which the NCA must respond and no response has been received.

8.7 Where the MLRO concludes that there are no reasonable grounds to suspect money laundering then she shall mark the report accordingly and give her consent for any ongoing or imminent transaction(s) to proceed.

8.8 All disclosure reports referred to the MLRO and reports made by her to the NCA must be retained by the MLRO in a confidential file kept for that purpose, for a minimum of five years.

8.9 The MLRO commits a criminal offence if she knows or suspects, or has reasonable grounds to do so, through a disclosure being made to him, that another person is engaged in money laundering and she does not disclose this as soon as practicable to the NCA.

9. Training

9.1 Officers considered likely to be exposed to suspicious situations, will be made aware of these by their senior officer and provided with appropriate training.

9.2 Additionally, all employees and Members will be familiarised with the legal and regulatory requirements relating to money laundering and how they affect both the Council and themselves.

9.3 Notwithstanding the paragraphs above, it is duty of officers and Members to report all suspicious transactions whether they have received their training or not.

10. Review

10.1 This policy will be reviewed annually.

This page is intentionally left blank

CONFIDENTIAL REPORTING (WHISTLEBLOWING) POLICY

Policy Statement

Version Control

Version No.	Author	Date
2.1	Kerry Beavis, Audit Manager	May 2020

Version 2.1
May 2020

CONFIDENTIAL REPORTING (WHISTLEBLOWING) POLICY

"North West Leicestershire District Council is committed to the prevention, deterrence, detection and investigation of fraud, corruption and malpractice in all forms. It encourages employees and members of the Council and its contractors who have serious concerns about any aspect of its work, including matters of health and safety, to voice those concerns."

1. INTRODUCTION

1.1 The Council is committed to the highest possible standards of openness, probity and accountability. In line with that commitment we expect employees, members and others that we deal with, who have serious concerns about any aspect of the Council's work to come forward and voice those concerns. This Confidential Reporting Policy is intended to encourage and enable employees, members, contractors or suppliers to raise serious concerns **within** the Council rather than overlooking a problem or "blowing the whistle" outside.

1.2 This Policy provides guidance on the way in which concerns may be raised.

This Policy also sets out how matters can be taken further if a person remains dissatisfied with the Council's response to any concerns raised.

1.3 Employees, members, contractors and suppliers are often the first to realise that there may be something seriously wrong within the Council. However, they may not express their concerns because they feel that speaking up would be disloyal to their colleagues or to the Council, or they perceive that it could harm their chances of future business or their career prospects. They may also fear harassment or victimisation. In such circumstances individuals may consider it to be easier to ignore the concern rather than report what may only be a suspicion of malpractice. This Policy document makes it clear that individuals raising concerns will do so without fear of victimisation, subsequent discrimination or disadvantage.

1.4 It is recognised that, where concerns are raised, most cases will have to proceed on a confidential basis. The Council will do everything it can to protect the confidentiality of those individuals raising concerns. However, there may be times when the person making the complaint can be identified due to the nature of the allegation made and in such cases it will not be possible to keep the identity of the complainant confidential. In addition, there may be times when the Council will believe it is appropriate to let the subject of a complaint know who made any allegation.

1.5 The Council recognises that individuals raising concerns, termed "qualifying disclosures" under the Public Interest Disclosure Act 1998 are entitled to protection under that Act and/or this Policy and may be eligible to compensation if they subsequently suffer victimisation, discrimination or disadvantage. Under the Enterprise and Regulatory Reform Act 2013, any disclosure using the Whistleblowing Policy, within reasonable belief of the worker making the disclosure will only be protected if it is made in the public interest. It must also show one or more of the following:

(a) that a criminal offence has been committed, is being committed or is likely to be committed,

(b) that a person has failed, is failing or is likely to fail to comply with any legal obligation to which he is subject,

(c) that a miscarriage of justice has occurred, is occurring or is likely to occur,

(d) that the health or safety of any individual has been, is being or is likely to be endangered,

(e) that the environment has been, is being or is likely to be damaged, or

(f) that information tending to show any matter falling within any one of the preceding paragraphs has been, is being or is likely to be deliberately concealed.

1.6 This policy is designed for workers. Workers include:

employees;
agency workers;
people that are training with an employer but not employed; and self-employed workers, if supervised or working off-site.

1.7 The procedures outlined in this Policy **are in addition to** the Council's complaints procedures and other statutory reporting procedures applying to some divisions.

1.8 This Policy has been discussed with the relevant trade unions and has their support.

1.9 The principles of this Policy also apply to concerns of the general public.

2. AIMS AND SCOPE OF THIS POLICY

2.1 This Policy aims to:

- encourage you to feel confident in raising concerns that are in the public interest and to question and act upon your concerns;
- provide avenues for you to raise those concerns and receive feedback on any action taken;
- ensure that you receive a response to your concerns and that you are aware of how to pursue matters if you are not satisfied;
- reassure you that you will be protected from the risk of reprisals or victimisation if you have a reasonable belief that you have made any disclosure in good faith.

2.2 If Council employees have concerns relating to their employment with the firm, these should be raised under the Council's Grievance Policy. This Policy is intended to cover major concerns that fall outside the scope of other policies and procedures. As stated in paragraph 1.5, these include:

- conduct which is an offence or a breach of law,
- disclosures related to miscarriages of justice,
- health and safety risks, including risks to the public as well as other employees,
- damage to the environment,
- the unauthorised use of public funds,
- possible fraud and corruption,
- sexual or physical abuse of clients, or
- other unethical conduct.

3. SAFEGUARDS - HARASSMENT OR VICTIMISATION

3.1 The Council is committed to good practice and high standards and aims to be supportive of employees and others using this Policy.

3.2 The Council recognises that the decision to report a concern can be a difficult one to make. You are legally entitled to protection from unfair treatment if:

(a) you honestly think what you are reporting is true,

(b) you believe that you are telling the right person,

(c) you believe that raising your concerns is in the public interest.

Put simply, if you are acting in good faith when raising any concerns, you should have nothing to fear because you will be doing your duty to your employer, and/or the Council and those for whom the Council provides a service. In the event that the concerns raised are substantiated, you will be ensuring that bad practice / unethical behaviour / illegal conduct is curtailed.

3.3 The Council will not tolerate any harassment or victimisation (including informal pressures) against individuals who raise concerns in good faith under this Policy and will take appropriate action to protect those who raise a concern in good faith and, where necessary, will take action against those subjecting any complainant to harassment, victimisation or any other pressures as a result of raising concerns.

3.4 Any investigation into allegations of matters listed in paragraph 2.2 of this Policy will not influence, or be influenced by, any disciplinary, redundancy or similar procedures which may already affect either the person raising the concerns or the individual(s) who are the subject of those concerns.

4. CONFIDENTIALITY

4.1 All attempts will be made to ensure any concerns raised will be treated in confidence and to protect your identity if you so wish. The Council cannot ensure your confidentiality if you have informed others of any alleged concerns.

4.2 In addition, there may be times when the identity of the person making the complaint is clear due to the nature of any allegations made. In such cases, the Council cannot take any steps to protect your identity. You will, however, still be entitled to the same protection against harassment, victimisation and other pressures as if your identity remained confidential.

4.3 In a small number of cases, the Council may find it is appropriate to disclose your identity to the person who is the subject of any complaint. It will, however, inform you of this before doing so. Again, you will receive the same protection against harassment, victimisation and other pressures as if your identity had remained confidential.

4.4 You should note that, whilst every effort will be made to protect your identity, the Council may, at an appropriate time ask you to come forward as a witness. If you do become a witness in any case, you will be entitled to the same protection against harassment, victimisation and other pressures that you are entitled to when making the initial complaint under this Policy.

5. ANONYMOUS ALLEGATIONS

5.1 This Policy aims to protect those raising concerns and, therefore, it is hoped that any person raising concerns will do so in their own name whenever possible.

5.2 Whilst any concern will be taken seriously, those expressed anonymously will carry less weight but will be given consideration by the Council; an investigation into the matters raised will be investigated at the discretion of the Council.

5.3 In exercising this discretion the factors to be taken into account will include:

- the nature and seriousness of the issues raised,
- the apparent credibility of the concern, and
- the probable likelihood of being able to confirm the allegation from attributable sources.

5.4 If the Council does not know who has made an allegation, it will not be possible for the Council to offer reassurance and protection to the individual.

6. UNTRUE ALLEGATIONS

6.1 If an allegation is made in good faith, but is not confirmed following an investigation by the Council, no action will be taken against the person making the allegation. This should encourage those who have concerns to raise it in the appropriate manner without fear of any reprisals.

6.2 If, however, an allegation is made frivolously, maliciously or for personal gain, disciplinary action may be taken against the person making that allegation where appropriate.

7. HOW TO RAISE A CONCERN

7.1 Advice and guidance on how to pursue matters of concern may be obtained from the Council's nominated contact points who are:

- Chief Executive: bev.smith@nwleicestershire.gov.uk
  Telephone 01530 454500
- Monitoring Officer: elizabeth.warhurst@nwleicestershire.gov.uk
  Telephone 01530 454762
- Section 151 Officer: tracy.bingham@nwleicestershire.gov.uk
  Telephone 01530 454707
- Audit Manager: lisa.marron@nwleicestershire.gov.uk
  Telephone 01530 454728

7.2 Concerns may be raised verbally or in writing, to any of the above named individuals. If raising a concern in writing, it should be addressed to the named individual at the:

Council Offices
North West Leicestershire District Council
Whitwick Road
Coalville
Leicestershire
LE67 3FJ

Clearly mark the envelope “Confidential”.

If you wish to make a written report you are invited to use the following format:

- the background and history of the concern (giving relevant dates);
- the reason why you are particularly concerned about the situation.

7.3 If you wish to make a verbal report of any concerns that you have identified, you are invited to contact one of the officers named at paragraph 7.1 above to arrange a mutually convenient appointment. When arranging an appointment, it would be helpful if you could mention that you would like to speak to them about a matter under the Confidential Reporting Policy.

7.4 When making a verbal report, you are invited to set out the facts using the same format identified at paragraph 7.2 above.

7.5 The earlier you express any concerns the easier it is for the Council to investigate and take any relevant action.

7.6 Although you are not expected to prove beyond doubt the truth of an allegation, you will need to demonstrate to the person contacted that there are reasonable grounds for your concern.

7.7 You may wish to consider discussing your concern with a colleague or trade union representative first and you may find it easier to raise the matter if there are two (or more) of you who share any concerns.

7.8 You may invite your trade union, professional association representative or a member of staff to be present during any meetings or interviews in connection with the concerns you have raised.

7.9 If you feel unable to raise your concerns directly with the Council, you should report the matter to a “prescribed person”. This will ensure that your legal rights are protected. The list of prescribed persons can change and so up to date information can be obtained by accessing an online brochure entitled “Whistleblowing: list of prescribed people and bodies-“ available at www.gov.uk.

8. HOW THE COUNCIL WILL RESPOND

8.1 The Council will respond to your concerns but within the constraints of maintaining confidentiality or observing any legal restrictions. In any event, a confidential record of the steps taken will be kept in accordance with the Data Protection Act 2018.

8.2 The Council may also ask to meet with you in order to gain further information from you. Do not forget that testing out your concerns is not the same as either accepting or rejecting them. It is sometimes necessary to test out any concerns raised in order to identify how strong any evidence may be.

8.3 Where appropriate, the matters raised may be:

- investigated internally,
- referred to the police,
- referred to the external auditor,
- made the subject of an independent enquiry.

Following any of the action above, a concern may be upheld or may be dismissed.

8.4 In order to protect individuals and those accused of misdeeds or possible malpractice, the Council will undertake initial enquiries to decide whether an investigation is appropriate and, if so, what form it should take. In most cases, it is anticipated that these initial enquiries will be completed within ten working days of an allegation being made. The overriding principle which the Council will have in mind when deciding what steps to take is whether the matter falls within the public interest. Any concerns or allegations which fall within the scope of any other specific procedures (for example, misconduct or discrimination issues) will normally be referred to the relevant service area for consideration under those procedures.

8.5 Some concerns may be resolved by agreed action without the need for investigation. If urgent action is required this will be taken before any investigation is conducted.

8.6 Within seven working days of a concern being raised, the nominated contact will write to you:

- acknowledging that the concern has been received,
- indicating how we propose to deal with the matter,
- giving an estimate of how long it will take to provide a final response,
- telling you whether any initial enquiries have been made,
- supplying you with information on staff support mechanisms, and
- telling you whether further investigations will take place and if not, why not.

8.7 The amount of contact between the officers considering the issues and you will depend on the nature of the matters raised, the potential difficulties involved and the clarity of the information provided. If necessary, the Council will seek further information from you.

8.8 Where any meeting is arranged, off-site if you so wish, you can be accompanied by a trade union or professional association representative or a friend.

8.9 The Council will take steps to minimise any difficulties which you may experience as a result of raising a concern. For instance, if you are required to give evidence in criminal or disciplinary proceedings the Council will arrange for you to receive advice about the procedure.

8.10 The Council accepts that you need to be assured that the matter has been properly addressed. Thus, subject to legal constraints, we will inform you of the outcome of any investigation.

9. THE RESPONSIBLE OFFICER

9.1 The Chief Executive has overall responsibility for the maintenance and operation of this Policy. That officer maintains a record of concerns raised and the outcomes (but in a form which does not endanger your confidentiality) and will immediately notify the Monitoring Officer and Section 151 Officer of all issues raised under this Policy and will report as necessary to the Council.

10. HOW THE MATTER CAN BE TAKEN FURTHER

10.1 This Policy is intended to provide you with an avenue within the Council to raise concerns. The Council hopes you will be satisfied with any action taken. If you are not, and if you feel it is right to take the matter outside the Council, the following are possible contact points:

- one of the “prescribed persons”
- your trade union
- your local Citizens Advice Bureau
- relevant professional bodies or regulatory organisations
- a relevant voluntary organisation (Public Concern at Work - 020 7404 6609)
- the Police.

10.2 If you take the matter outside the Council, you should ensure that you do not disclose confidential information. Check with one of the Council’s nominated contact points about that (see 7.1).

11. Review

11.1 This policy will be reviewed bi-annually and whenever the relevant legislation changes.

This page is intentionally left blank

RISK MANAGEMENT POLICY

Policy Statement

Version Control

Version No.	Author	Date
1		December 2014
2		May 2016
3	Andy Barton	May 2020

May 2020

RISK MANAGEMENT POLICY

1. INTRODUCTION

1.1 The Council has adopted the principles of risk management in order to meet the following objectives:

- to protect the health, safety and welfare of its employees and the communities it serves;
- to protect its property, assets and other resources;
- to protect the services it provides; to main its reputation and good standing in the wider community; and
- to deliver its overall objectives and priorities.

2. RISK MANAGEMENT STRUCTURE

2.1 Risk Management is co-ordinated corporately by the Health and Safety Officer and through the Corporate Risk Scrutiny Group (RSG) chaired by a Strategic Director. It also refers and reports to Corporate Leadership Team thereby reaching all services in the Council and ensuring senior management oversight and involvement. Progress on Corporate Risk Management will be reported to members through performance reports to the Audit and Governance Committee. The Corporate Portfolio Holder is the Cabinet member with overall responsibility for risk management, the Leader of the Council.

2.2 Risk management is embedded in the culture of the authority through:

- the continued adoption of the Council's risk management policy statement;
- a nominated officer lead, currently the Head of HR and Organisation Development;
- the Corporate Risk Scrutiny Group and Corporate Leadership Team accountability;
- an established uniform procedure for the identification, analysis, management and monitoring of risk;
- training and briefings in conjunction with appropriate third parties and
- regular monitoring and reporting through the corporate performance management system and control mechanisms.

2.3 The Council is responsible for establishing and maintaining appropriate risk management processes, control systems, accounting records and governance arrangements. Internal Audit play a vital role in advising the Council that these arrangements are in place and operating effectively. Each year the Audit Manager produces a risk-based annual Audit Plan. This is informed by a risk assessment which includes a review of corporate and service risk registers, and consultation with key stakeholders and senior management. The Plan is developed to deliver a programme of internal audits to provide independent assurance to senior management and members. Internal audit undertake a risk based approach for individual assignments and gives a rating of the level of assurance that be awarded within each system / business area. This demonstrates the extent to which controls are operating effectively to ensure that significant risks to the achievement of the Council's priorities are being addressed.

3. AIMS OF THE POLICY

3.1 The Council will strive to maintain its diverse range of services to the community and visitors to the North West Leicestershire area. It will protect and continue to provide

these services by ensuring that its assets, both tangible and intangible, are protected against loss and damage. The Council is committed to a programme of risk management to ensure its ambitions for the community can be fulfilled through:

"The identification, analysis, management and financial control of those risks which can most impact on the Council's ability to pursue its approved delivery plan".

3.2 The Council is committed to using risk management to maintain and improve the quality of its own services as well as any contribution by partnerships through its community leadership role. The Risk Management Policy has the following aims and objectives:

- to continue to embed risk management into the culture of the Council;
- to promote the recognition of risk within the Council's defined corporate aims and objectives;
- continue to raise risk awareness within the Council and its partners;
- to manage risk in accordance with best practice;
- to comply with legislation and guidance;
- to improving safety and increase safety awareness;
- to protect Council property, services and public reputation;
- to reduce disruption to services by having effective contingency or recovery plans in place to deal with incidents when they occur;
- to minimise injury, damage, loss and inconvenience to residents, staff, service users, assets, etc arising from or connected with the delivery of Council services;
- to review robust frameworks and procedures for the identification, analysis, assessment and management of risk, and the reporting and recording of events, based on best practice;
- to maximise value for money.

3.3 Regularly through the Risk Scrutiny Group, the Council's Corporate Leadership Team (CLT) will review the Risk Management Policy and its risk management processes to ensure their continued relevance to the Council. The annual review will also assess performance against the aims and objectives set out above. Completion of the self-evaluation matrix will be a key monitoring tool and a central part of this review. CLT will be accountable to members for the effective management of risk within the Council. This will be achieved through the quarterly reporting of corporate risks to Audit and Governance Committee and Cabinet.

4. RISK MANAGEMENT POLICY

4.1 The overall objective of the Council's risk management Policy is to ensure that risks to the Council's objectives, services, employees, partnerships and contractors are identified, recorded, amended, prioritised and then addressed by being treated, tolerated, transferred or terminated. The Policy incorporates:

(a) <u>Identification / Consideration of Risks</u>

- Identifies corporate and operational risks, assesses the risks for likelihood and impact, identifies mitigating controls and allocates responsibility for the mitigating controls.
- Requires the consideration of risk within all service plans and reviews and the regular review of existing risks as identified in the risk register.
- Requires, reports supporting strategic policy decisions and project initiation documents, to include a risk assessment.

- Externally horizon scan for impending risks that may impact the council, communicate the risk to the appropriate risk owner so they can assess for likelihood and impact, identify mitigating controls and allocate responsibility for the mitigating controls.

(b) Development Delivery

- Allocates responsibility for embedding risk management to a senior officer and Member, to jointly champion.
- Embeds risk management into; strategic planning, financial planning, policy making and review, and performance management.
- Requires that an update report arising from the work of the Risk Scrutiny Group is presented to Corporate Leadership Team for discussion and information on a quarterly basis.
- Develops arrangements to monitor and measure performance of risk management activities against the Council's strategic aims and priorities.
- Considers risks in relation to significant partnerships, which requires assurances to be obtained about the management of those risks.

(c) Member Involvement / Responsibility

- Quarterly reports will be produced for Audit and Governance Committee on the management of business risks together with recommendation of appropriate actions.
- Reporting to Cabinet and Portfolio members.

(d) Training / Awareness

- Requires relevant training and tool kits to be given to appropriate staff to enable them to take responsibility for managing risks within their environment.
- Requires the maintenance of documented procedures for the control of risk and the provision of suitable information, training and supervision.
- Develops appropriate procedures and guidelines.
- Considers positive risks (opportunities) and negative risks (threats).
- Facilitates risk management awareness training for all members.

(e) Review

- Maintains and reviews a register of corporate business risks linking them to strategic business objectives and assigning ownership for each risk.
- Requires an annual review of the risk management process, including a report to CLT, localised Risk Registers where necessary and quarterly reporting to the Audit and Governance Committee.
- In the case of new or changing strategic risks, report to Audit and Governance Committee and/or Cabinet through the quarterly performance reporting process.
- Requires each team / department to review their individual Risk Registers as and when required (but no less than quarterly).

(f) Business Continuity

- Develops contingency plans in areas where there is a potential for an occurrence having a catastrophic effect on the delivery of the Council's services.

(g) Insurance

- Ensures the appropriate officer responsible for insurance is notified of any new risks.
- Ensures adequate records are maintained and retained to support the Council's defence against disputed insurance claims.

(h) Controlling the Risks

Traditionally in risk management there are four ways to mitigate the risks to the organisation, these being typically referred to as **Treat, Tolerate, Transfer and Terminate** and are known collectively as the "4 Ts".

- **Tolerate** means the risk is known and accepted by the organisation. In such instances the senior management team should formally sign off that this course of action has been taken.
- **Transfer** means the risk mitigation is transferred i.e. it is passed to a third party such as an insurer or an outsourced provider, although it should be noted that responsibility for the risk cannot be transferred or eliminated.
- **Terminate** means we stop the process, activity, etc or stop using the premises, IT system, etc which is at risk and hence the risk is no longer relevant.
- **Treat** means we aim to reduce the likelihood of the threat materialising or else reduce the resultant impact through introducing relevant controls and continuity strategies.

5. CORPORATE RISK SCRUTINY GROUP

5.1 The Corporate Risk Scrutiny Group is made up of technical experts and corporate leads from the Council's Service Areas. Members of the Group act as "champions" for risk within their services and the Group provides a link into the CLT.

5.2 The role of the Group is to maintain a formal framework that will assist with the management of risk and business continuity, by developing the corporate lead and advising CLT on the expected outcome. The objectives of the Group are:

- to assess and advise on the reduction of prevailing risks within the Council's services, to the benefit of staff and the public;
- to discuss, agree and recommend as appropriate, on matters relating to corporate risk policy;
- to make reports and recommendations to CLT;
- to discuss operational risks insofar as they relate to matters of cross-directorate interest;
- to oversee the implementation of the Council's risk management Policy, and to promote a holistic approach to its ongoing management;
- to promote good risk management practices with the aim of reducing potential liabilities;
- to consider and identify new risks, and ideas / schemes for risk reduction;
- to provide a forum to discussion on risk management issues.

These will be achieved through the following:

- the use of the Council's Risk Management reporting system;
- monitoring the Risk Management Policy;
- reviewing the Council's risk register and associated action plans, acting as a forum for examining and rating risks and making recommendations to CLT;

- developing a comprehensive performance framework for risk management, and developing and using key indicators capable of showing improvements in risk management and providing early warning of risk;
- supporting the development and review of internal standards and procedures regarding significant risk areas;
- supporting the development and implementation of relevant training, awareness and education programmes;
- supporting the development and implementation of adequate, relevant and effective reporting, communication and information dissemination systems with managers and staff;
- supporting the effective monitoring and review of near misses, untoward incidents and accidents, legal and insurance claims and verifying that appropriate management action has been taken promptly to minimise the risk of future occurrence;
- supporting the review of the risk register and action plans to ensure that appropriate management action is taken appropriately to tolerate, treat, transfer or terminate the risk;
- monitoring compliance with legal and statutory duties;
- providing progress reports to CLT and members, drawing to their attention significant business risks;
- encouraging localised Risk Registers to be created where necessary, as well as supporting dynamic risk assessment.

6. PROCEDURES

6.1 The Council will adopt uniform procedures for the identification, analysis, management and monitoring of risk. These will be embodied in a formal risk management framework, which will be subject to annual review by the Audit and Governance Committee, following consideration by CLT.

The approved framework is set out in Appendix A to this Policy document.

7. FUNDING FOR RISK MANAGEMENT

7.1 The annual Service and Financial Planning process will include a review of operational risks and consider the allocation of funds for risk management initiatives as part of the annual budget process. If additional funds are required approval will be sought initially from CLT.

8. BENEFITS OF EFFECTIVE RISK MANAGEMENT

8.1 Effective risk management will deliver a number of tangible and intangible benefits to Individual services and to the Council as a whole e.g.

<u>Improved Strategic Management</u>

- Greater ability to deliver against objectives and targets
- Increased likelihood of change initiatives being delivered effectively
- Improved reputation, hence support for regeneration
- Increased confidence to take controlled risks

<u>Improved Operational Managements</u>

- Reduction in interruptions to service delivery: fewer surprises!

- Reduction in managerial time spent dealing with the consequences of a risk event occurring
- Improved health and safety of employees and others affected by the Council's activities
- Compliance with legislation and regulations

Improved Financial Management

- Better informed financial decision-making
- Enhanced financial control
- Reduction in the financial costs associated with losses due to service interruption, litigations, etc.
- Improved containment of insurance premiums

Improved Customer Service

- Minimal service disruption to customers and a positive external image

APPENDIX A

RISK MANAGEMENT FRAMEWORK

(A) What is the framework?

This framework promotes a set of uniform risk management procedures through which directorates will identify, analyse, monitor and manage the risks faced by the Council.

For the purposes of the framework, risk management is defined as *"the identification, analysis, management and financial control of those risks that can impact on the Council's ability to deliver its services and priorities."*

Risk management is therefore concerned with better decision making, through a clear understanding of all associated risks before final decisions are made by either members or officers. When risks are properly identified, analysed and prioritised it is possible to formulate action plans that propose management actions to reduce risk or deal adequately with the consequences of the risks should they occur. The underlying aim is to treat, terminate or transfer risk to bring them to an acceptable manageable level within the Council, monitor tolerated risk, ensuring services to the public can be maintained, and that the Council's priorities can be fulfilled.

Risk management therefore supports the Council's service planning process by positively identifying the key issues that could affect the delivery of the service objectives.

(B) Why does the Council need to consider risk management as part of its service planning?

All organisations have to deal with risks, whatever their nature. As a general principle the Council will seek to reduce or control all risks that have the potential to:

- harm individuals;
- affect the quality of service delivery or delivery of the council's priorities;
- have a high potential of occurrence;
- would affect public confidence;
- would have an adverse effect on the council's public image;
- would have significant financial consequences;
- have a potential for litigation in line with exposure detailed below.

Risk Management cannot therefore be considered in isolation, but needs to be an integral part of decision-making and service planning processes of the Council. Risk management must be fully embedded in:

- service planning,
- performance management,
- best value,
- committee reports.

For this reason risk management is located within the HR and Organisation Development team of the Council, with high level commitment by the Chief Executive to integrate risk management in everything the Council does.

(C) Assessing risk

Once risks have been identified, an assessment of their significance is required. This requires a robust and transparent scoring mechanism to be used uniformly across Council directorates.

Scoring should be a group exercise including managers and frontline employees. This is because people's perceptions vary and this can have an effect on scoring the risk. Employees who experience a risk every day can become complacent and fail to see how serious it may actually be, whilst a group will usually see the wider impact.

A decision on risk ownership is also required. The owner should be at management level and be responsible for ensuring that controls identified to manage the risk are in place and that they are effective. Delegation of responsibility for particular actions to other employees is acceptable, but overall control of risk must remain with management.

Tables 1 and 2 below set out a scoring mechanism for assessing the likelihood and the impact of exposure to risk.

Table 1 - assessing the likelihood of exposure

1. Low	Likely to occur once in every ten years or more
2. Medium	Likely to occur once in every two to three years
3. High	Likely to occur once a year
4. Very High	Likely to occur at least twice in a year

Table 2 - assessing the impact of exposure

1. Min or	Loss of a service for up to one day. Objectives of individuals are not met. No injuries. Financial loss over £1,000 and up to £10,000. No media attention. No breaches in Council working practices. No complaints / litigation.
2. Medium	Loss of a service for up to one week with limited impact on the general public. Service objectives of a service unit are not met. Injury to an employee or member of the public requiring medical treatment. Financial loss over £10,000 and up to £100,000. Adverse regional or local media attention - televised or news paper report. Potential for a complaint litigation possible. Breaches of regulations / standards.

3. Serious	Loss of a critical service for one week or more with significant impact on the general public and partner organisations. Service objectives of the directorate of a critical nature are not met. Non-statutory duties are not achieved. Permanent injury to an employee or member of the public Financial loss over £100,000. Adverse national or regional media attention - national newspaper report. Litigation to be expected. Breaches of law punishable by fine.
4. Major	An incident so severe in its effects that a service or project will be unavailable permanently with a major impact on the general public and partner organisations. Strategic priorities of a critical nature are not met. Statutory duties are not achieved. Death of an employee or member of the public. Financial loss over £1m. Adverse national media attention - national televised news report. Litigation almost certain and difficult to defend. Breaches of law punishable by imprisonment.

(D) Prioritisation of risk

Table 3 brings together in a matrix the likelihood and impact of risk.

Table 3 - a risk matrix

		Likelihood			
		1	**2**	**3**	**4**
Impact	**4**	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4

Based on this matrix, the Council must decide on the level of risk it is prepared to accept as part of its ongoing operations. Any risk above the agreed level should be considered unacceptable and will therefore need to be managed. The risks in the above matrix fall into three zones; red, amber and green. Table 4 sets out the Councils intended response to these risks.

Table 4 - intended responses to risk

Red	Controls and/or mitigating actions are required to reduce the risk to an acceptable level. Effort should be focused on reducing the risk of any items appearing in this zone, hence moving them to the amber or green zone.
Amber	Risks will require ongoing monitoring to ensure they do not move into the red zone. Depending on the resources required to address

	the red risks, it may be appropriate to develop controls/mitigating actions to control these risks.
Green	Existing controls and/or mitigating actions are sufficient and may be excessive. More resource committed to reduce these risks is likely to be wasted. Consideration should be given to relaxing the level of control to release resources for mitigating higher level risks.

(E) Format of the risk register

Annex 1 to this framework provides a standard format.

Corporate Risk Register													
	Risk Description	Consequence	Cause	Inherent Risk			Responsibility of	Responsible to	Control Measures	Residual Risk			
Ref No.				Impact	Likelihood	Rating				Impact	Likelihood	Rating	Movement of Risk

This page is intentionally left blank

CORPORATE POLICY AND PROCEDURE ON THE REGULATION OF INVESTIGATORY POWERS ACT 2000 AND THE INVESTIGATORY POWERS ACT 2016

Version Control

Date	Action
December 2006	ASG Revised
May 2009	ASG Reviewed
June 2010	AW Reviewed and updated
March 2012	ASG Revised
October 2012	HO Guidance issued
September 2013	RH Reviewed and updated
October 2015	DMG Reviewed and updated
9 December 2015	Approved by Audit and Governance Committee
12 January 2016	Approved by Council

June 2020

CORPORATE POLICY AND PROCEDURE ON THE REGULATION OF INVESTIGATORY POWERS ACT 2000 AND THE INVESTOGATORY POWERS ACT 2016

1. INTRODUCTION

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) is concerned with the regulation of surveillance and other intelligence gathering by public authorities in the conduct of their legitimate business.

1.2 The Investigatory Powers Act 2016 (IPA) sets out the extent to which certain investigatory powers may be used to interfere with privacy. In particular about the interception of communications, equipment interference and the acquisition and retention of **communications data**.

1.3 Section 6 of the Human Rights Act 1998 provides that it is unlawful for a public authority to act in a way which is incompatible with a European Convention right. Article 8 of the European Convention on Human Rights says that everyone has the right to respect for their private and family life, their home and their correspondence.

1.4 The use of surveillance and other intelligence gathering techniques may amount to an interference with rights protected by Article 8 of the European Convention on Human Rights and could amount to a violation of those rights unless the interference is in accordance with the law.

1.5 The aim of RIPA and the IPA is to provide a balance between preserving people's right to privacy and enabling enforcement agencies to gather evidence for effective enforcement action. RIPA provides a statutory framework for the authorisation of certain types of **covert** intelligence gathering which is consistent with the Human Rights Act 1998 and the European Convention on Human Rights. Similarly, the IPA provides a statutory framework for the lawful interception and use of **communications data**.

1.6 The Council has approved a policy for tackling fraud and corruption. In limited circumstances the Council may wish to use surveillance techniques or **communications data** for the purpose of enforcing this policy or other of its statutory functions. The requirements of RIPA and the IPA are most likely to apply to those sections of the Council with enforcement / investigatory functions.

1.7 Section 27 of RIPA provides that conduct authorised under RIPA will be "lawful for all purposes." This means a person authorised under RIPA is entitled to engage in the conduct which has been authorised under RIPA and the Council will be protected from challenges to both the gathering of, and the subsequent use of, covertly obtained information enabling the Council to show that it has acted lawfully.

1.8 RIPA also provides a statutory mechanism for authorising the use of a "**covert human intelligence source**", e.g. undercover agents.

1.9 The IPA permits access to **communications data** in specific circumstances.

1.10 Non-compliance with RIPA or the IPA may result in:

1.10.1 evidence being disallowed by the courts;

1.10.2 a complaint to the Investigatory Powers Commissioner's Office;

1.10.3 a complaint to the Local Government and Social Care Ombudsman; and/or

1.10.4 the Council being ordered to pay compensation.

It is essential therefore that the Council's policies and procedures, as set out in this document, are followed. A flowchart of the procedures to be followed is at Appendix 1.

2. TYPES OF SURVEILLANCE

2.1 Surveillance includes monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications. It also includes recording any of the aforementioned activities.

2.2 Surveillance may be "**overt**" or "**covert**".

2.3 Surveillance will be "**overt**" if the act of surveillance is not calculated to be hidden from view, even if the motives of the person undertaking the surveillance remain concealed.

2.4 Most of the surveillance carried out by the Council is done overtly – there is nothing secretive, clandestine or hidden about it. In many cases, officers will be behaving in the same way as a normal member of the public, and/or will be going about Council business openly. Similarly, surveillance will be **overt** if the subject has been told it will happen (e.g. where a noisy householder is warned that noise will be recorded if it continues).

2.5 Surveillance is "**covert**" if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place. RIPA regulates two types of **covert** surveillance.

2.6 The first type of **covert** surveillance is "**directed surveillance**". "**Directed surveillance**" means surveillance that is:

2.6.1 **covert**;

2.6.2 not intrusive;

2.6.3 undertaken for the purposes of a specific investigation or specific operation;

2.6.4 undertaken in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

2.6.5 undertaken otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under RIPA to be sought for the carrying out of the surveillance.

2.7 RIPA states that "**private information**" includes any information relating to a person's private or family life. The Home Office Covert Surveillance and Property Interference Revised Code of Practice (latest edition at time of writing was August 2018) states that as a result, "**private information**" is capable of including any aspect of a person's private or personal relationship with others, such as family (which should be treated as extending beyond the formal relationships created by marriage or civil partnership) and professional or business relationships.

2.8 RIPA sets out a number of grounds on which an authorisation for **directed surveillance** can be considered necessary. In the case of a Local Authority, only one of these grounds is applicable, that ground is that **directed surveillance** is necessary "for the purpose of preventing or detecting crime or of preventing disorder".

2.9 The fact that **covert** surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will usually result in the obtaining of private information about that person as well as others that he or she comes into contact or associates with.

2.10 An example of **directed surveillance** would be when officers follow a person over a period of time to find out whether they are working at the same time as claiming benefit. Similarly, although town centre CCTV cameras will not normally require a RIPA authorisation, if a camera is directed in such a way as to observe a particular individual, this would amount to **directed surveillance** and an authorisation would be required.

2.11 The second type of **covert** surveillance is "**intrusive surveillance**". Surveillance is intrusive if, and only if, it is **covert** surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

2.12 A Local Authority cannot carry out **intrusive surveillance** under RIPA. **Intrusive surveillance** can only be carried out by the police and other law enforcement agencies.

3. CONDUCT AND USE OF COVERT HUMAN INTELLEGENCE SOURCES

3.1 A person is a **Covert Human Intelligence Source** (**CHIS**) if he or she establishes or maintains a personal or other relationship with another person in order to covertly obtain or disclose information.

3.2 RIPA sets out special rules relating to the management and use of information supplied by a **CHIS** and a duty of care is owed to the **CHIS** in how the information is used.

3.3 The conduct or use of a **CHIS** requires prior authorisation. Again, the ground on which a **CHIS** may be used by a Local Authority is "for the purpose of preventing or detecting crime or of preventing disorder."

3.4 A RIPA authorisation may not be required in circumstances where members of the public volunteer information to the Council as part of their normal civic responsibilities, however, this will depend on how the information has been obtained. If the person has obtained the information as an 'insider' i.e. in the course of a personal or other relationship or "as a result of the existence of such a relationship" then the person is likely to be a **CHIS** even if the relationship was not formed or maintained for that purpose.

3.5 If the person has obtained the information as an outside observer then he or she is not a **CHIS**.

3.6 Where contact numbers are set up by the Council to receive information then it is unlikely that persons reporting information will be **CHISs** and similarly, people who complain about anti- social behaviour, and are asked to keep a diary, will not normally

be **CHISs** because they are not being required to establish or maintain a relationship for a **covert** purpose.

Juvenile CHISs

3.7 Special safeguards apply to the use or conduct of juveniles, that is, those under 18 years old, as a **CHIS**. On no occasion should the use or conduct of a **CHIS** under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for them. In other cases, authorisations should not be granted unless the special provisions, contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (as amended), are satisfied.

3.8 Authorisations for juvenile sources should be granted by those listed in the table at Annex A of the Home Office Covert Human Intelligence Sources Revised Code of Practice (latest edition at time of writing was August 2018). In this Council, only the Chief Executive may authorise the use of a juvenile or vulnerable individual as a CHIS. The duration of such an authorisation is four months from the time of grant or renewal (instead of twelve months), and the authorisation should be subject to at least monthly review. For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.

4. OPEN SOURCE (ONLINE) COVERT ACTIVITY

4.1 The use of the internet may be required to gather information during an operation, which may amount to **directed surveillance**. The Home Office Covert Surveillance and Property Interference Revised Code of Practice (latest edition at time of writing was August 2018) advises that simple reconnaissance of websites, that is, preliminary examination with a view to establishing whether a site or its contents are of interest, is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a **directed surveillance** authorisation. However, where there is an intention to use the internet as part of an investigation and private information is likely to be obtained, a RIPA authorisation should be considered. When conducting an investigation which involves the use of the internet factors to consider are:

- officers must not create a false identity in order to "befriend" individuals on social networks without an authorisation under RIPA;
- officers viewing an individual's public profile on a social network should do so only to the minimum degree necessary and proportionate in order to obtain evidence to support or refute the suspicions or allegations under investigation;
- repeated viewing of open profiles on social networks to gather evidence or to monitor an individual's status, must only take place once a RIPA authorisation has been granted and approved by a Magistrate; and
- officers should be aware that it may not be possible to verify the accuracy of information on social networks and, if such information is to be used as evidence, take reasonable steps to ensure its validity.

4.2 Further, where an investigator may need to communicate covertly online, for example, contacting individuals using social media websites without disclosing his or her identity, a **CHIS** authorisation should be considered.

5. USE OF PERSONAL DEVICES FOR BUSINESS USE

5.1 Using of a personal device to access the internet or social media for business use, for example, as part of investigation, is still captured by RIPA. Consequently, officers are advised not to use personal devices for business use particularly using a personal device to access the internet and social media for business use.

6. THE COUNCIL OWNED DRONE

6.1 Use of a drone has the potential to capture **private information**. **Collateral intrusion** is also highly likely when using a drone. Therefore, consideration should be given to whether a RIPA authorisation is required. A drone can be a very useful tool to use in an investigation, however, if used to gather **personal information** the subject of the surveillance will either need to be notified of the use of the drone (such that any surveillance is not **covert**) or a RIPA authorisation will be needed.

6.2 If the drone is to be used for publicity purposes, consideration must be given to the area the drone will be used and/or the event at which the drone will be used. The Council should avoid using the drone in residential areas as this is likely to capture **private information**. If this is not possible, residents should be notified in advance and consideration should be given to obtaining a RIPA authorisation. If the drone is to be used at public events, this should be made clear on any communications advertising the event.

7. LOCAL AUTHORIY DIRECTED SURVEILLANCE CRIME THRESHOLD

7.1 A **Crime Threshold** applies to the authorisation of **directed surveillance** by Local Authorities under RIPA (see article 7A of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010). This **Crime Threshold** does not apply to the authorisation of a **CHIS** by a Local Authority.

7.2 Local Authorities can only authorise use of **directed surveillance** under RIPA for the purpose of preventing or detecting criminal offences or disorder associated with criminal offences that are:

7.2.1 punishable, whether on summary conviction or on indictment, by a maximum term of at least six months imprisonment; or

7.2.2 relate to the underage sale of alcohol or tobacco.

7.3 If the **Crime Threshold** is not met, though surveillance is still required, a Non-RIPA form should be completed. A Non-RIPA form requires the applicant officer to consider necessity and proportionality as per a RIPA authorisation, however, there is no requirement for approval by a Justice of the Peace.

8. AUTHORISATION PROCESS - DIRECTED SURVEILLANCE AND USE OF A CHIS

<u>Stage 1 - Request for Authorisation</u>

8.1 **Directed surveillance** or the use of a **CHIS** can only be authorised by a Local Authority if the authorisation is *necessary* for the purpose of preventing or detecting crime or preventing disorder and the authorised surveillance is *proportionate* to what is sought to be achieved by carrying the surveillance out. When authorising the use of a **CHIS** arrangements also need to be in place for management of the **CHIS** and to ensure the security and welfare of the **CHIS**.

8.2 For **directed surveillance** or the use of a **CHIS**, only the approved RIPA forms, available on the Home Office website

(https://www.gov.uk/government/collections/ripa-forms--2)

may be used. Any other form will be rejected by the Authorising Officer. The applicant officer should complete the appropriate form providing as much detail as possible then submit to the appropriate Authorising Officer for authorisation.

8.3 If in doubt about the process to be followed or the information required in the form, an applicant officer should always seek the advice of the Head of Legal and Commercial Services or the Audit Manager before applying for an authorisation under RIPA.

8.4 The applicant officer will be responsible for ensuring that copies of all forms are forwarded to the Audit Manager within seven days of issue. As a control measure the Audit Manager will supply the applicant officer with a referenced copy of the authorisation which they should keep in their department in secure storage. Officers should ensure that material passing between them is sent in such a way that it cannot be read or intercepted by other people.

Stage 2 - Considering an Application for Authorisation

8.5 **Directed surveillance** or use of a **CHIS** can only be lawfully carried out if properly authorised and carried out in strict accordance with the terms of the authorisation.

8.6 The Secretary of State has specified by statutory instrument (the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010) that, for any district council in England, Directors, Heads of Service or Service Managers or equivalent are designated persons for the purpose of s.28 and s.29 of RIPA, that is, they may act as Authorising Officers for the purpose of authorising applications for **directed surveillance** or the use of a **CHIS**. In this Council, the Chief Executive and the Directors are designated to act as Authorising Officers under the Constitution (Part 3, Sec 7, Para 3.3). The Chief Executive or Directors may designate other officers to act as Authorising Officers, provided these officers are of the level specified by the Secretary of State in the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (i.e. Heads of Service can be designated as Authorising Officers).

8.7 Before signing a form seeking authorisation, the Authorising Officer must have regard to this Policy and Procedure, to any relevant Code of Practice, to any advice from the Head of Legal and Commercial Services or the Audit Manager and to any other relevant guidance.

8.8 The Authorising Officer must also satisfy himself / herself that the surveillance proposed in the application is:

8.8.1 in *accordance with the law*;

8.8.2 *necessary* in the circumstances of the particular case on the ground of preventing or detecting crime or preventing disorder; and

8.8.3 *proportionate* to what it seeks to achieve.

8.9 In considering whether or not the proposed surveillance is proportionate, the Authorising Officer will need to consider:

8.9.1 The seriousness of the crime or disorder which the surveillance seeks to detect and weigh this against the type and extent of surveillance proposed. For minor offences, it may be that surveillance is never proportionate; and

8.9.2 whether there are other more non- intrusive ways of achieving the desired outcome. If there are none, the Authorising Officer will need to consider whether the proposed surveillance is no more than necessary to achieve the objective, as the least intrusive method will be considered proportionate by the courts.

8.10 The Authorising Officer will also need to take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance. This is known as "**collateral intrusion**". Measures must be taken whenever practicable to avoid or minimise, so far as practicable, **collateral intrusion**.

8.11 When authorising the conduct or use of a **CHIS** the Authorising Officer must also be satisfied that appropriate arrangements are in place for the management and oversight of the **CHIS**. This must address health and safety issues through a risk assessment. The Authorising Officer must also have regard to any adverse impact on community confidence that may result from the use or conduct of the information obtained.

8.12 The authorisation does not take effect until a Justice of the Peace has made an order approving the grant of the authorisation.

Stage 3 - Judicial Approval

8.13 If the Authorising Officer is satisfied that the surveillance is *necessary* and *proportionate* they will instruct Legal Services to seek approval from a Justice of the Peace sitting at the Magistrates' Court.

8.14 Legal Services will request a hearing date from the Court. The time taken to obtain a heating date from the Court will need to be taken into account when scheduling any proposed surveillance.

8.15 Urgent approvals should not be necessary.

8.16 If the approval is urgent and cannot be handled the next working day then the applicant officer should:

8.16.1 phone the Court's out of hours legal staff contact. You will be asked about the basic facts and urgency of the authorisation. If the police are involved in the investigation you will need to address why the police cannot authorise the application.

8.16.2 If urgency is agreed, then arrangements will be made for a suitable Magistrate to consider the application. You will be told where to attend and give evidence.

8.16.3 Attend the hearing as directed with two copies of the signed RIPA authorisation form.

8.17 At the hearing the Council will provide the Court with a copy of the authorisation signed by the Authorising Officer, together with any supporting documents relevant to the matter showing the necessity and proportionality of the authorisation and which contain all the information relied upon. Also included will be a summary of the circumstances of the case.

8.18 The hearing will be in private heard by a single Justice of the Peace (Magistrate / District Judge) who will read and consider the application.

8.19 On reviewing the papers and hearing the application the Justice of the Peace will determine whether they are satisfied that there were, at the time the authorisation was granted, and continue to be reasonable grounds for believing that the authorisation is *necessary* and *proportionate*. In addition they must also be satisfied that the Authorising Officer had the relevant authority to authorise the Council's own internal authorisation prior to it passing to the Court.

8.20 For authorisations for the use of a **CHIS** the Justice of the Peace will also need to be satisfied that there were and are reasonable grounds for believing appropriate arrangements are in place for the management and oversight of the **CHIS**.

8.21 The Justice of the Peace may ask questions of the Council in order to satisfy themselves of the necessity and proportionality of the request.

8.22 In considering the application the Justice of the Peace may decide to:

8.22.1 grant an Order approving the authorisation or renewal. The authorisation or renewal will then take effect and the Local Authority may proceed to use surveillance in accordance with the authorisation;

8.22.2 refuse to approve the authorisation or renewal. The RIPA authorisation will not take effect and the Local Authority may not use the proposed surveillance. Where an application has been refused the Council may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the need to go through the internal authorisation process again. The Council may then wish to reapply for judicial approval once those errors have been remedied;

8.22.3 refuse to approve the grant or renewal and quash the authorisation or notice. A Justice of the Peace must not exercise its power to quash an authorisation unless the applicant (the Council) has had at least two business days' notice from the date of the refusal in which to make representations.

Stage 4 - Duration and Review

8.23 If the Justice of the Peace approves the authorisation, the authorisation will last, in the case of **directed surveillance**, a period of three months and, in the case of a **CHIS**, a period of 12 months.

8.24 Authorising Officers must then conduct regular reviews of authorisations granted in order to assess the need for the surveillance to continue. Reviews should be conducted on a monthly basis as a minimum. The Authorising Officer may decide that reviews should be conducted more frequently, particularly where a high level of collateral intrusion is likely.

8.25 A review involves consultation with the applicant officer and any other persons involved in the surveillance. The applicant officer must give sufficient information about the surveillance and any information obtained by the surveillance for the Authorising Officer to be satisfied that the authorised surveillance should continue. Applicant officers should be pro-active in preparing reports to assist Authorising Officers carry out reviews.

Stage 5 - Renewals

8.26 If it appears that the surveillance will continue to be *necessary* and *proportionate* beyond the three month period for **directed surveillance** or 12 months for use of a **CHIS**, the authorisation must be renewed.

8.27 An application for renewal should be made by the applicant officer by completing the appropriate form which is available from the Home Office website (https://www.gov.uk/government/collections/ripa-forms--2). This form should then be submitted to the Authorising Officer who must then consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred.

8.28 The Authorising Officer must be satisfied that it is *necessary* and *proportionate* for the authorisation to continue and that the **Crime Threshold** continues to be met. The authorisation for renewal must then be approved by a Justice of the Peace for it to take effect.

8.29 An authorisation may be renewed and approved before the initial authorisation ceases to have effect but the renewal takes effect from the time at which the authorisation would have expired. If necessary, a renewal can be granted more than once.

Stage 6 - Cancellations

8.30 The Authorising Officer who granted or last renewed the authorisation must cancel the authorisation if the grounds for granting (or renewing) no longer apply or if the authorisation is no longer *necessary* or *proportionate*.

8.31 An authorisation can be cancelled on the initiative of the Authorising Officer following a periodic review or after receiving an application for cancellation from the applicant officer. Forms for the cancellation of **directed surveillance** and use of a **CHIS** are available on the Home Office website

(https://www.gov.uk/government/collections/ripa-forms--2)

9. COMMUNICATIONS DATA

9.1 The term "**communications data**" includes the "who", "when", "where", and "how" of a communication but not the content i.e. what was said or written. It includes the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning, of the communication.

9.2 It can include the address to which a letter is sent, the time and duration of a communication, the telephone number or e-mail address of the originator and recipient, and the location of the device from which the communication was made. It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services.

9.3 The acquisition of **communications data** is permitted under Part 3 of the IPA and will be a justifiable interference with an individual's human rights under the European Convention on Human Rights only if the conduct being authorised or required to take

place is *necessary* for the purposes of a specific investigation or operation, *proportionate* and *in accordance with law*.

9.4 Training should be made available to all those who participate in the acquisition and disclosure of **communications data**.

9.5 The Home Office has published the "Communications Data Code of Practice" (latest edition at time of writing was November 2018). This code should be readily available to persons involved in the acquisition of **communications data** under the IPA and persons exercising any functions to which this code relates must have regard to the code.

9.6 The IPA stipulates that conduct to be authorised must be *necessary* for one or more of the purposes set out in the IPA. For Local Authorities this purpose is "for the applicable crime purpose" which means:

9.6.1 where the **communications data** is wholly or partly events data (events data covers information about time-bound events taking place across a telecommunication system at a time interval, for example, information tracing the origin or destination of a communication that is, or has been, in transmission), the purpose of preventing or detecting serious crime; or

9.6.2 in any other case, the purpose of preventing or detecting crime or of preventing disorder.

9.7 "Serious Crime" means:

9.7.1 an offence for which an adult is capable of being sentenced to one year or more in prison;

9.7.2 any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal;

9.7.3 any offence committed by a body corporate;

9.7.4 any offence which involves the sending of a communication or a breach of privacy; or

9.7.5 an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy.

9.8 A Local Authority may not make an application that requires the processing or disclosure of internet connection records for any purpose.

10. AUTHORISATION PROCESS - COMMUNICATIONS DATA

10.1 Acquisition of **communications data** under the IPA involves four roles:

10.1.1 The Applicant Officer - The applicant officer is a person involved in conducting or assisting an investigation or operation within a relevant public authority who makes an application in writing or electronically for the acquisition of **communications data**;

10.1.2 The Single Point of Contact (SPoC) - The SPoC is an individual trained to facilitate the lawful acquisition of **communications data** and effective co-operation between a public authority, the Office for Communications Data Authorisations (OCDA) and telecommunications operators and postal operators. To become accredited an

individual must complete a course of training appropriate for the role of a SPoC and have been issued the relevant SPoC unique identifier. The Home Office provides authentication services to enable telecommunications operators and postal operators to validate SPoC credentials;

10.1.3 The Senior Responsible Officer - Within every relevant public authority there should be a Senior Responsible Officer. The Senior Responsible Officer must be of a senior rank in a public authority. This must be at least the same rank as the designated senior officer specified in Schedule 4 of the IPA. Where no designated senior officer is specified the rank of the senior responsible officer must be agreed with the Home Office. In this Council the Senior Responsible Officer is the Chief Executive; and

10.1.4 The Authorising Individual - **Communications data** applications can be authorised by three separate categories of individual depending on the circumstances of the specific case. The Authorising Individual for Local Authorities is the authorising officer in the OCDA. Section 60A of the IPA confers power on the IPC to authorise certain applications for **communications data**. In practice the IPC will delegate these functions to his staff. These staff will sit in a body which is known as the OCDA.

10.2 An authorisation provides for persons within a public authority to engage in conduct relating to a postal service or telecommunication system, or to data derived from such a telecommunication system, to obtain **communications data**. The following types of conduct may be authorised:

10.2.1 conduct to acquire **communications data** - which may include the public authority obtaining **communications data** themselves or asking any person believed to be in possession of or capable of obtaining the **communications data** to obtain and disclose it; and/or

10.2.2 the giving of a notice - allowing the public authority to require by a notice a telecommunications operator to obtain and disclose the required data.

<u>Stage 1 - Making an Application</u>

10.3 Before public authorities can acquire **communications data**, authorisation must be given by an Authorising Individual. An application for that authorisation must include an explanation of the necessity of the application.

10.4 Necessity should be a short explanation of the investigation or operation, the person and the **communications data** and how these three link together. The application must establish the link between the three aspects to be able to demonstrate the acquisition of **communications data** is necessary for the statutory purpose specified.

10.5 When granting an authorisation the authorising individual must also believe that conduct to be proportionate to what is sought to be achieved by obtaining the specified **communications data** – that the conduct is no more than is required in the circumstances. This involves balancing the extent of the interference with an individual's rights and freedoms against a specific benefit to the investigation or operation being undertaken by a relevant public authority in the public interest.

10.6 As well as consideration of the rights of the individual whose data is to be acquired consideration must also be given to any actual or potential infringement of the privacy and other rights of individuals who are not the subject of the investigation or operation.

10.7 The applicant officer will complete an application form setting out for consideration the necessity and proportionality of a specific requirement for acquiring **communications data**.

10.8 The application should record subsequently whether it was authorised by an authorising individual and when that decision was made. Applications should be retained by the public authority and be accessible to the SPoC.

Stage - 2 Consultation with the Single Point of Contact

10.9 A SPoC must be consulted on all Local Authority applications before they are authorised.

10.10 Amongst other things the SPoC will:

10.10.1 assess whether the acquisition of specific **communications data** from a telecommunications operator or postal operator is reasonably practicable or whether the specific data required is inextricably linked to other data; and

10.10.2 advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of telecommunications operators or postal operators.

10.11 The National Anti-Fraud Network ('NAFN') is hosted by Tameside Metropolitan Borough Council.

10.12 In accordance with section 73 of the IPA, all Local Authorities who wish to acquire **communications data** under the IPA must be party to a collaboration agreement. In practice this means they will be required to become members of NAFN and use NAFN's shared SPoC services. Applicant officers within Local Authorities are therefore required to consult a NAFN SPoC throughout the application process. The accredited SPoCs at NAFN will scrutinise the applications independently. They will provide advice to the Local Authority ensuring it acts in an informed and lawful manner.

10.13 In addition to being considered by a NAFN SPoC, the local authority making the application must ensure someone of at least the rank of the senior responsible officer in the local authority is aware the application is being made before it is submitted to an authorising officer in OCDA. The local authority senior responsible officer must be satisfied that the officer(s) verifying the application is (are) of an appropriate rank and must inform NAFN of such nominations. In this Council the Chief Executive is the Senior Responsible Officer and the officers notified to the NAFN (notified in March 2019) as able to verify applications are the Head of Legal and Commercial Services and the Audit Manager.

10.14 NAFN will be responsible for submitting the application to OCDA on behalf of the local authority.

Stage 3 - Authorisation of Applications

10.15 The (OCDA) performs this function on behalf of the IPC. An authorising officer in OCDA can authorises requests from Local Authorities.

10.16 The authorising individual is responsible for considering and, where appropriate, authorising an application for **communications data**. It is their responsibility to consider the application and record their considerations at the time, in writing or

electronically in order to show that they have understood the need for the application and considered necessity and proportionality to a standard that will withstand scrutiny. Comments should be tailored to a specific application as this best demonstrates the application has been properly considered.

10.17 If the authorising individual believes the acquisition of **communications data** meets the requirements set out in the IPA and is necessary and proportionate in the specific circumstances, an authorisation will be granted. If the authorising individual does not consider the criteria for obtaining the data have been met the application should be rejected and/or referred back to the SPoC and the applicant officer.

Stage 4 - Refusal to Grant an Authorisation

10.18 Where a request is refused by an authorising officer in OCDA, the public authority has three options:

10.18.1 not proceed with the request;

10.18.2 resubmit the application with a revised justification and/or a revised course of conduct to acquire **communications data**; or

10.18.3 resubmit the application with the same justification and same course of conduct seeking a review of the decision by OCDA. A public authority may only resubmit an application on the same grounds to OCDA where the senior responsible officer or a person of equivalent grade in the public authority has agreed to this course of action. OCDA will provide guidance on its process for reviewing such decisions.

Stage 5 - Duration of Authorisations and Notices

10.19 An authorisation becomes valid on the date upon which the authorisation is granted. It is then valid for a maximum of one month. This means the conduct authorised should have been commenced, which may include the giving of a notice, within that month.

10.20 Any notice given under an authorisation remains in force until complied with or until the authorisation under which it was given is cancelled.

10.21 All authorisations should refer to the acquisition or disclosure of data relating to a specific date(s) or period(s). Any period should be clearly indicated in the authorisation. The start date and end date should be given, and where a precise start and end time are relevant these must be specified.

10.22 Where an authorisation relates to the acquisition or obtaining of specific data that will or may be generated in the future, the future period is restricted to no more than one month from the date upon which the authorisation was granted.

10.23 Authorising individuals should specify the shortest possible period of time for any authorisation. To do otherwise would impact on the proportionality of the authorisation and impose an unnecessary burden upon the relevant telecommunications operator(s) or postal operator(s).

Stage 6 - Renewal of Authorisations

10.24 Any valid authorisation may be renewed for a period of up to one month by the grant of a further authorisation. A renewed authorisation takes effect upon the expiry of the authorisation it is renewing.

10.25 Renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future. The reasons for seeking renewal should be set out by the applicant officer in an addendum to the application upon which the authorisation being renewed was granted.

10.26 Where an authorising individual is granting a further authorisation to renew an earlier authorisation, they should:

10.26.1 consider the reasons why it is necessary and proportionate to continue with the acquisition of the data being generated; and

10.26.2 record the date and, when appropriate to do so, the time when the authorisation is renewed.

Stage 7 - Cancellations

10.27 An authorisation may be cancelled at any time by the Local Authority or OCDA and must be cancelled if, at any time after the granting of the authorisation, it is no longer necessary for a statutory purpose or the conduct required by the authorisation is no longer proportionate to what was sought to be achieved.

10.28 In practice, it is likely to be the public authority that is first aware that the authorisation is no longer necessary or proportionate. In such cases the SPoC (having been contacted by the applicant officer, where appropriate) must cease the authorised conduct.

10.29 A notice given under an authorisation (and any requirement imposed by a notice) is cancelled if the authorisation is cancelled but is not affected by the authorisation ceasing to have effect at the end of one month period of validity.

11. CENTRAL CO-ORDINATION

11.1 The Chief Executive will be the Senior Responsible Officer for the overall implementation of RIPA and the IPA.

11.2 The Head of Legal and Commercial Services will be responsible for:

11.2.1 giving advice and assistance to all staff concerned with the operation of RIPA and the IPA;

11.2.2 arranging training for all staff concerned with the operation of RIPA and the IPA; and

11.2.3 maintaining and keeping up to date this corporate policy and procedure.

11.3 The Audit Manager will be responsible for:

11.3.1 maintaining a central and up to date record of all authorisations;

11.3.2 along with the Head of Legal and Commercial Services, giving advice and assistance to all staff concerned with the operation of RIPA and the IPA; and

11.3.3 allocating reference numbers to authorisations.

12. WORKING WITH OTHER AGENCIES

12.1 When another agency has been instructed on behalf of the Council to undertake any action under RIPA, this Council will be responsible for obtaining a RIPA authorisation and therefore this Policy and Procedure must be used. The other agency must then be given explicit instructions on what actions it may undertake and how these actions are to be undertaken.

12.2 When another agency (e.g. Police, HMRC, etc):

12.2.1 wish to use the Council's resources (e.g. CCTV surveillance systems) for RIPA purposes, that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes he or she must obtain a copy of that agency's RIPA form, a copy of which must be passed to the Audit Manager for inclusion on the central register;

12.2.2 wish to use the Council's premises for their own RIPA action, and is expressly seeking assistance from the Council, the request should normally be granted unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the other agency's activities. Suitable insurance or other appropriate indemnities may need to be sought. In such cases, the Council's own RIPA forms should not be used as the Council is only assisting and not involved in the RIPA activity of the other agency.

13. OTHER SOURCES OF INFORMATION

13.1 The Home Office has issued Codes of Practice on **directed surveillance**, **CHISs** and **communications data**. These Codes of Practice supplement this policy and procedure document and should be used as a source of reference by all officers whose task it is to apply the provisions of RIPA and the IPA and their subordinate legislation.

14. RECORDS MANAGEMENT

14.1 The Council must keep a detailed record of all authorisations, judicial approvals, reviews, renewals, cancellations and rejections in the relevant services. A central record of all authorisation forms, whether authorised or rejected, will be maintained and monitored by the Audit Manager.

14.2 All Authorising Officers must send all original applications for authorisation to the Audit Manager. Each document will be given a unique reference number, the original will be placed on the central record and a copy will be returned to the applicant officer.

14.3 Copies of all other forms used and the judicial approval form must be sent to the Audit Manager bearing the reference number previously given to the application to which it refers.

Service Records

14.4 Each service must keep a written record of all authorisations issued to it, and any judicial approvals granted, to include the following:

14.4.1 a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;

14.4.2 a record of the period over which the operation has taken place;

14.4.3 the frequency of reviews prescribed by the Authorising Officer;

14.4.4 a record of the result of each review;

14.4.5 a copy of any renewal of an authorisation and any supporting documentation submitted when the renewal was requested;

14.4.6 the date and time when any instruction was given by the Authorising Officer, including cancellation of such authorisation;

14.4.7 a copy of the order approving or otherwise the grant or renewal of an authorisation from a Justice of the Peace; and

14.4.8 the required date of destruction and when this was completed.

Central Record Maintained by the Audit Manager

14.5 A central record of all authorisation forms, whether authorised or rejected, is kept by the Audit Manager. The central record must be readily available for inspection on request by the Investigatory Powers Commissioner.

14.6 The central record must be updated whenever an authorisation is granted, reviewed, renewed or cancelled. Records will be reviewed after a period of 6 years from the date on which the relevant criminal or civil proceedings file is closed for archive and deleted when no longer necessary.

14.7 The central record must contain the following information:

14.7.1 the type of authorisation;

14.7.2 the date on which the authorisation was given;

14.7.3 name / rank of the Authorising Officer;

14.7.4 details of attendances at the Magistrates' Court to include date of attendances at court, the determining Justice of the Peace, the decision of the Justice of the Peace and the time and date of that decision;

14.7.5 the unique reference number (URN) of the investigation / operation. This will be issued by the Audit Manager when a new application is entered in the Central Record. The applicant officer will be informed accordingly and should use the same URN when requesting a renewal or cancellation;

14.7.6 the title of the investigation / operation, including a brief description and names of the subjects, if known;

14.7.7 if the authorisation was renewed, when it was renewed and who authorised the renewal, including the name and rank / grade of the Authorising Officer;

14.7.8 whether the investigation / operation is likely to result in the obtaining of **confidential information** (information is confidential if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an

obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, information from a patient's medical records; or matters subject to legal privilege);

14.7.9 if the authorisation was reviewed, when it was reviewed and who authorised the review, including the name and rank / grade of the Authorising Officer;

14.7.10 the date and time that the authorisation was cancelled.

14.8 It should also contain a comments section enabling oversight remarks to be included for analytical purposes.

14.9 The Audit Manager co-ordinating RIPA and IPA applications ensures that there is an awareness of the investigations taking place. This would also serve to highlight any unauthorised **covert** surveillance being conducted.

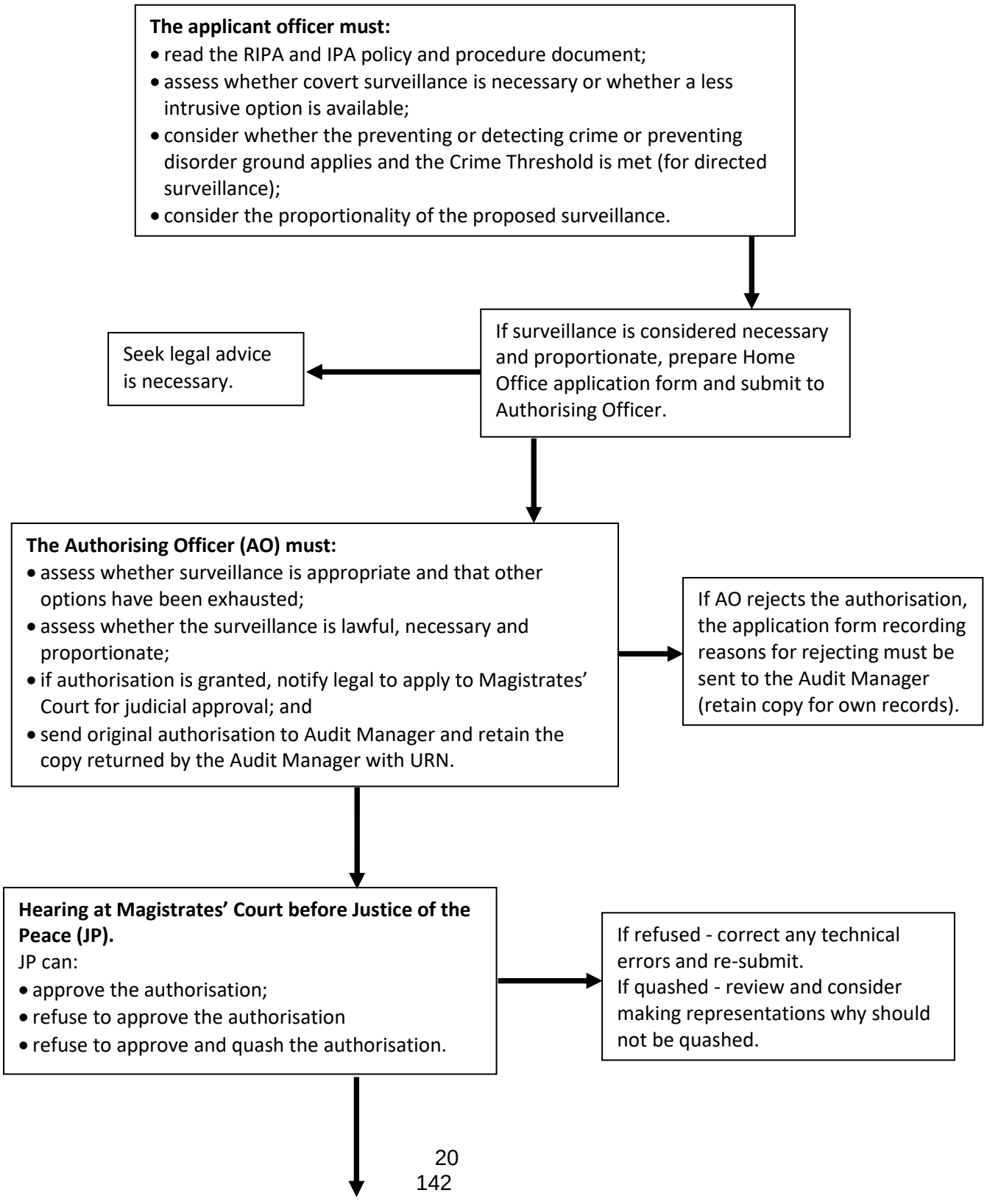
Retention and Destruction of Material

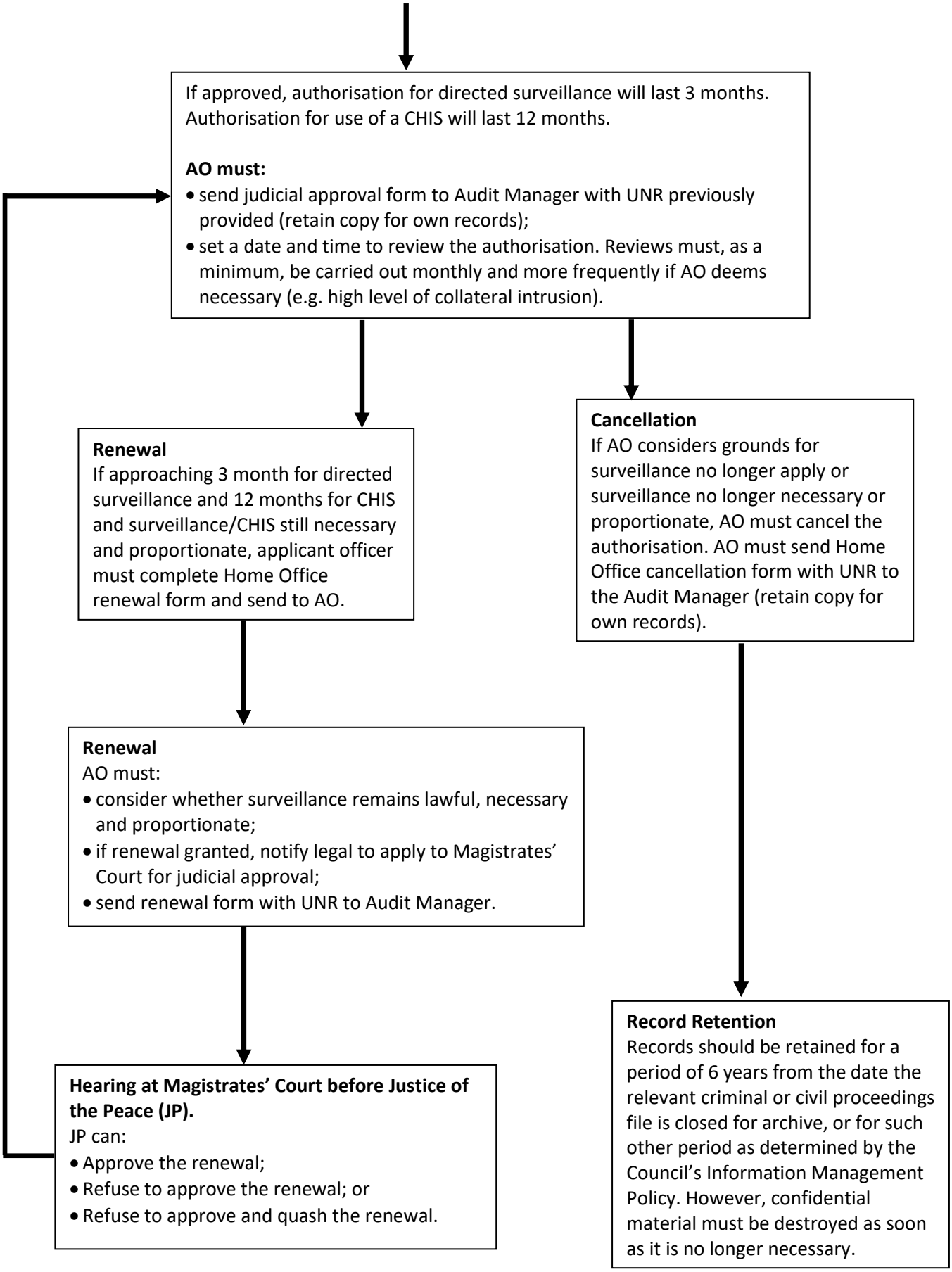
14.10 Departments must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of **covert** surveillance, a CHIS and/or the acquisition of communications data which accord with the Council's Information Management Policy. Records will be reviewed after a period of 6 years from the date on which the relevant criminal or civil proceedings file is closed for archive and must be destroyed as soon as they are no longer necessary. **Confidential material must be destroyed as soon as it is no longer necessary**. It must not be retained or copied unless it is necessary for a specified purpose. Where there is doubt, advice must be sought from the Head of Legal and Commercial Services or the Senior Responsible Officer.

APPENDIX 1

RIPA - AUTHORISATION OF DIRECTED SURVEILLANCE / USE OF A CHIS PROCEDURE

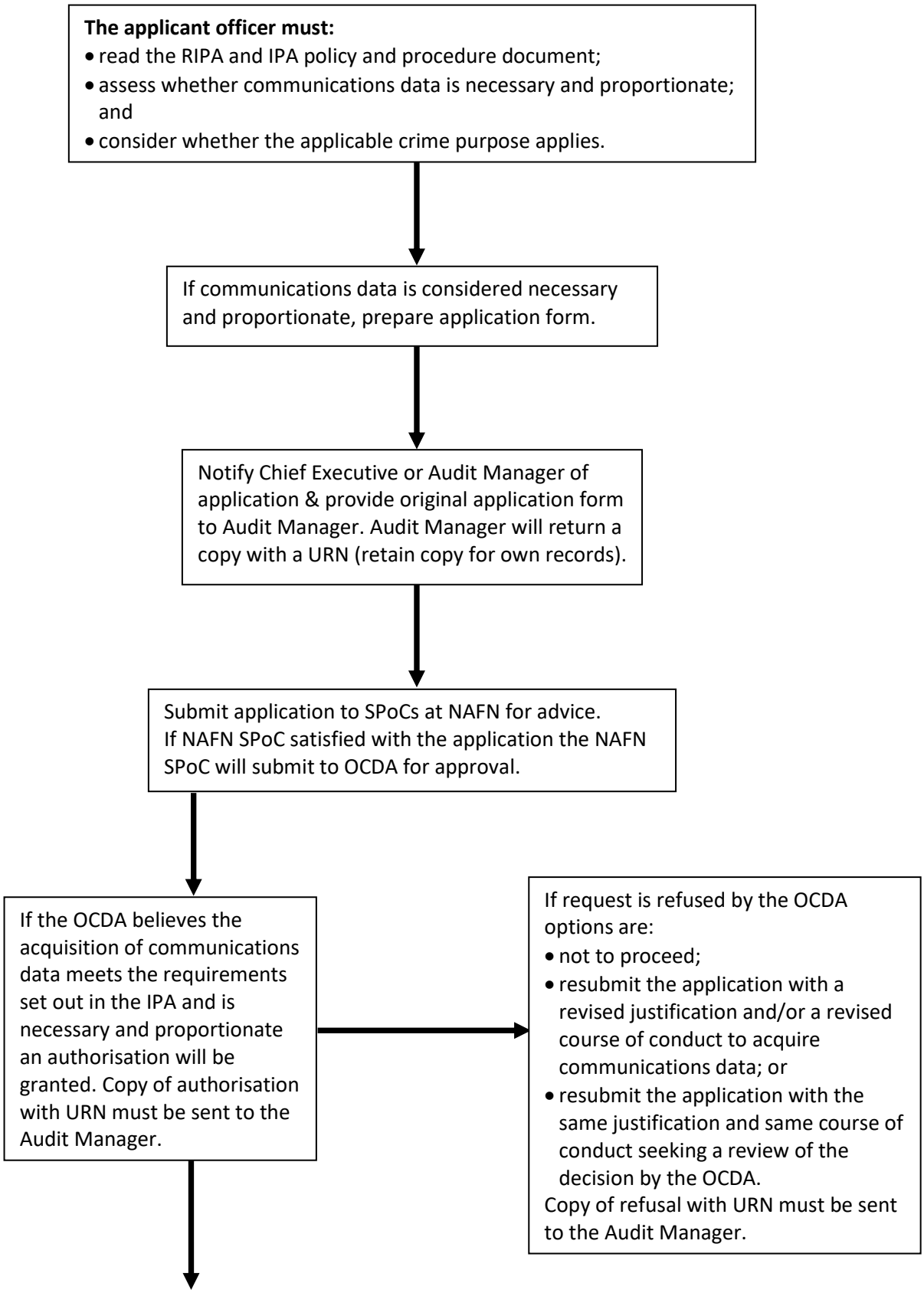
(Note: Note: Only the Chief Executive may authorise the use of a juvenile or vulnerable individual as a CHIS)

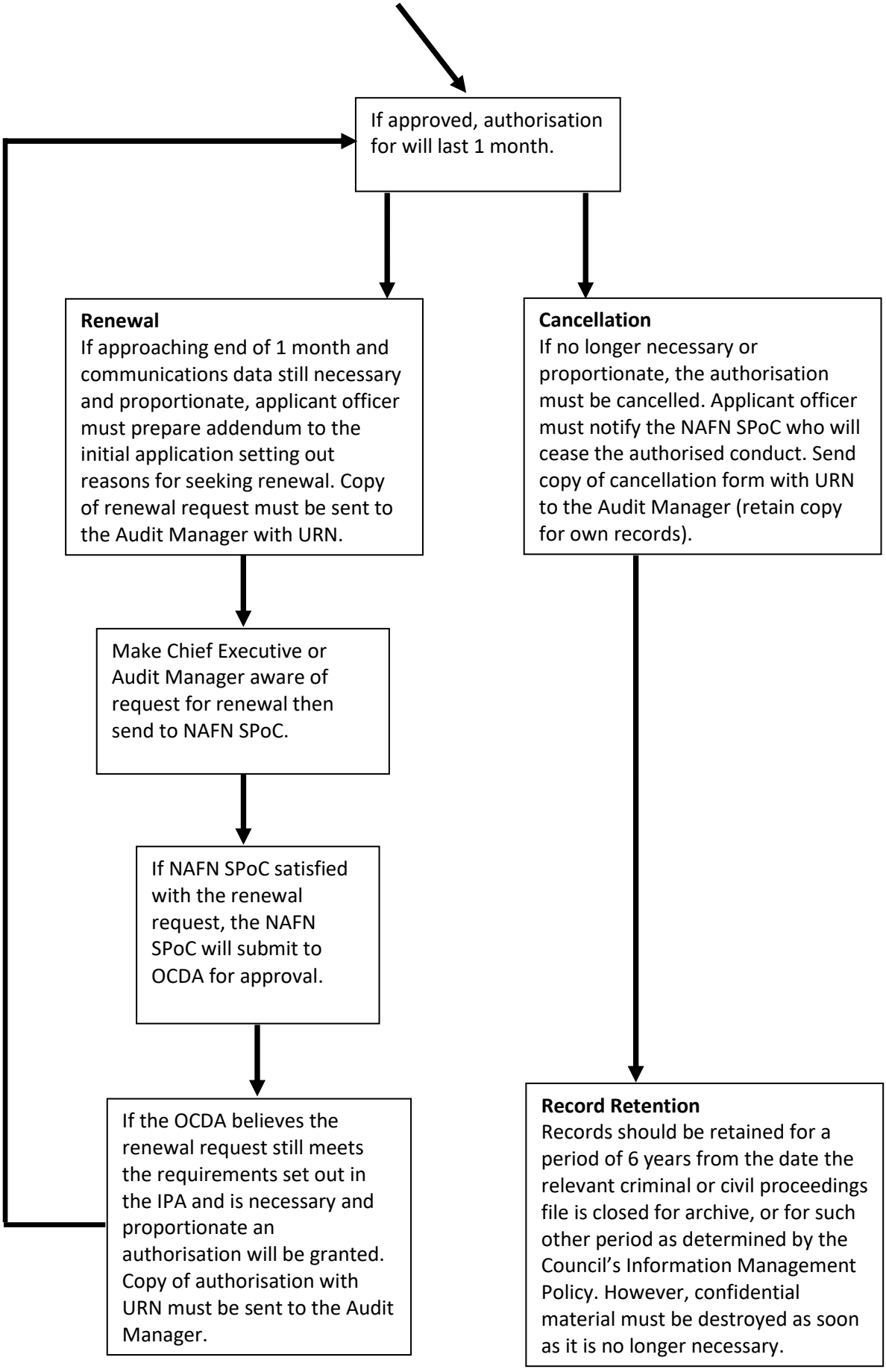



If approved, authorisation for directed surveillance will last 3 months. Authorisation for use of a CHIS will last 12 months.
AO must:
• send judicial approval form to Audit Manager with UNR previously provided (retain copy for own records);
• set a date and time to review the authorisation. Reviews must, as a minimum, be carried out monthly and more frequently if AO deems necessary (e.g. high level of collateral intrusion).
Renewal
If approaching 3 month for directed surveillance and 12 months for CHIS and surveillance/CHIS still necessary and proportionate, applicant officer must complete Home Office renewal form and send to AO.
Cancellation
If AO considers grounds for surveillance no longer apply or surveillance no longer necessary or proportionate, AO must cancel the authorisation. AO must send Home Office cancellation form with UNR to the Audit Manager (retain copy for own records).
Renewal
AO must:
• consider whether surveillance remains lawful, necessary and proportionate;
• if renewal granted, notify legal to apply to Magistrates' Court for judicial approval;
• send renewal form with UNR to Audit Manager.
Hearing at Magistrates' Court before Justice of the Peace (JP).
JP can:
• Approve the renewal;
• Refuse to approve the renewal; or
• Refuse to approve and quash the renewal.
Record Retention
Records should be retained for a period of 6 years from the date the relevant criminal or civil proceedings file is closed for archive, or for such other period as determined by the Council's Information Management Policy. However, confidential material must be destroyed as soon as it is no longer necessary.

APPENDIX 1

IPA - COMMUNICATIONS DATA AUTHORISATION PROCESS




If approved, authorisation for will last 1 month.
Renewal
If approaching end of 1 month and communications data still necessary and proportionate, applicant officer must prepare addendum to the initial application setting out reasons for seeking renewal. Copy of renewal request must be sent to the Audit Manager with URN.
Cancellation
If no longer necessary or proportionate, the authorisation must be cancelled. Applicant officer must notify the NAFN SPoC who will cease the authorised conduct. Send copy of cancellation form with URN to the Audit Manager (retain copy for own records).
Make Chief Executive or Audit Manager aware of request for renewal then send to NAFN SPoC.
If NAFN SPoC satisfied with the renewal request, the NAFN SPoC will submit to OCDA for approval.
If the OCDA believes the renewal request still meets the requirements set out in the IPA and is necessary and proportionate an authorisation will be granted. Copy of authorisation with URN must be sent to the Audit Manager.
Record Retention
Records should be retained for a period of 6 years from the date the relevant criminal or civil proceedings file is closed for archive, or for such other period as determined by the Council's Information Management Policy. However, confidential material must be destroyed as soon as it is no longer necessary.

This page is intentionally left blank

INFORMATION MANAGEMENT POLICY

Version Control

Version No.	Author	Date	Update Information
V1.0	Lynn Wyeth	20.11.2015	Original Draft
V1.1	Lynn Wyeth	04.12.2015	Amendments by NWLDC incorporated
V1.2	Lee Mansfield	15.12.2015	Amendment made following CLT decision - SIRO
V1.3	Lee Mansfield	02.02.2016	To reference legal as location of the IM team
V1.4	Sabrina Doherty	23.02.2017	Changes made to team structures, functions, roles and responsibilities
V1.5	Andrew Hickling / Louis Sebastian	09.05.2018	Changes made to team structures, functions, roles and responsibilities
V1.6	Nicola Taylor / Mackenzie Keatley	01.07.2020	Change made to team structures, roles and responsibilities, training and support, legislation update

June 2020

INFORMATION MANAGEMENT POLICY

POLICY STATEMENT

"Information is a vital corporate asset of the Council which is of extremely high value. North West Leicestershire District Council is committed to ensuring that information is efficiently managed and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management."

1. INTRODUCTION

1.1 The key areas of Information Management are:

- Records Management;
- Information Risk;
- Information Security;
- Environmental Information Regulations 2004;
- Freedom of Information Act 2000;
- Data Protection Act 2018;
- General Data Protection Regulations;
- Local Government Transparency Code 2015;
- Privacy and Electronic Communication Regulations;
- Public Services Network Code of Connection;
- Payment Card Industry Security Standards;
- Confidentiality.

1.2 This policy is part of a set of information management policies and procedures that support the delivery of an Information Management framework, and should be read in conjunction with these associated documents, listed at section 4.

2. PURPOSE OF THE POLICY

2.1 This Information Management policy provides an overview of the Councils approach to information management, a guide to the procedures in use, and details about the management structures within the organisation.

2.2 This policy enables the Council to ensure that all information is dealt with legally, fairly, securely, efficiently, and effectively.

2.3 This policy ensures that the provisions of the Freedom of Information Act 2000 (FOI), the Environmental Information Regulations 2004 (EIRs), the Data Protection Act 2018 (DPA), the General Data Protection Regulation (GDPR) and the Public Services Network Code (PSN CoCo) are complied with.

3. SCOPE OF THIS POLICY

3.1 This policy, framework and supporting policies apply to:

- all information systems within the organisation (both electronic and paper based);
- all data, information, and records owned by the Council, but also including those held by contractors or partner organisations on behalf of, or as a result of their relationship with, the Council);

- any information that is owned by other organisations, but may be accessed and used by Council employees;
- information in whatever storage format and however transmitted (i.e., paper, voice, photo, video, audio or any digital format. It will also cover formats that are developed and used in the future.);
- all employees of the Council, Council members, temporary workers, volunteers, student placements, etc;
- the employees of any other organisations having access to Council information, for example, auditors, contractors, and other partner agencies where there is no specific information sharing protocol in place,

3.2 The procedures outlined in this Policy are in addition to the Council's complaints procedures and other statutory reporting procedures applying to some divisions.

3.3 This Policy has been discussed with the relevant trade unions and has their support.

4. PROCEDURES AND GUIDANCE

4.1 This Information Management Policy will be strengthened by other associated Council policies / procedures / material including but not limited to:

- ICT Security Policy;
- Request for Information Procedure;
- Security Incident Procedure;
- Records Management Procedure;
- Information Sharing Procedure;
- Whistleblowing Policy;
- RIPA Policy;
- Anti-Money Laundering Policy;
- Employment Practices Code - Information Commissioner's Office.

5. PRINCIPLES OF INFORMATION MANAGEMENT

5.1 The Council understands the need for an appropriate balance between openness and confidentiality in the management and use of information. The Council also understands the need to share information with others in a controlled manner.

5.2 To maximise the value of organisational assets the Council will endeavour to ensure that data is:

- held securely and confidentially;
- obtained fairly and lawfully;
- recorded accurately and reliably;
- used effectively and ethically;
- shared and disclosed appropriately and lawfully;

5.3 To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental, the Council will ensure:

- information will be protected against unauthorised access;
- confidentiality of information will be assured;
- integrity of information will be maintained;
- information will be supported by the highest quality data;

- regulatory and legislative requirements will be met;
- business continuity plans will be produced, maintained and tested;
- information security training will be mandatory for all staff;
- all breaches of information security, actual or suspected, will be reported via the Security Incident Procedure and investigated by the Data Protection Officer or Information Management Officer;
- significant breaches will be handled with support from Human Resources and/or ICT Manager and/or Legal Services;

6. ROLES AND RESPONSIBILITIES

6.1 Information Asset Owners

6.1.1 Information Asset Owners (IAOs) are Heads of Service who are the nominated owners for one or more identified information assets within the Council. Their role is to understand what information is held, added, removed, how information is moved and who has access and why.

6.1.2 Information Asset Owners will:

- know what information comprises or is associated with the asset, and understand the nature and justification of information that flows to and from the asset;
- know who has access to the asset, whether system or information, why access is required, and ensures access is monitored and compliant with policy;
- understand and address risks to the asset, providing assurance to the Senior Information Risk Owner;
- ensure there is a legal basis for processing data and for any disclosures made;
- refer queries about any of the above to the Information Governance Team.

6.2 Senior Information Risk Owner

6.2.1 From 1 July 2016 the Head of Legal and Commercial Services will become the SIRO.

The SIRO will report to the CLT on all matters relating to Information Management. The SIRO is an executive who is familiar with and takes ownership of the organisation's information risk policy, and acts as advocate for information risk.

6.3 Data Protection Officer

6.3.1 As of the 4 November 2018 the Council appointed a Data Protection Officer.

Under GDPR it is mandatory that a public authority appoint a Data Protection Officer (DPO).

The DPO's tasks are defined in Article 39 of the GDPR.

The DPO Information Management responsibilities include:

- implementing information management procedures and processes for the organisation;
- raising awareness about information management to all staff;
- ensuring that training is provided annually and is completed by all staff;

- co-ordinating the activities of any other staff given responsibilities for data protection, confidentiality, information quality, records management and Freedom of Information;
- conducting internal audits to ensure compliance on an ad-hoc basis;
- ensures the Council is responsible for the continued integrity of datasets and maintains and enforces applications of policies and standards;
- to co-operate with the supervisory authority (ICO).

6.4 Information Governance

6.4.1 Information management is co-ordinated and managed by the Information Governance Team. The Team will:

- assist the Senior Information Risk Owner in the implementation of their key responsibilities and any other matters as deemed appropriate and necessary;
- maintain an awareness of information management issues within the Council;
- review and update the information management policy in line with local and national requirements;
- review and audit all procedures relating to this policy where appropriate on an ad-hoc basis;
- ensure that line managers are aware of the requirements of the policy.

6.5 ICT Team Manager

6.5.1 The ICT Team Manager is responsible for:

- the formulation and implementation of ICT related policies and the creation of supporting procedures;
- developing, implementing and managing robust ICT security arrangements in line with best industry practice, legislation, and statutory requirements;
- effective management and security of the Council's ICT infrastructure and equipment;
- developing and implementing a robust IT Disaster Recovery Plan;
- ensuring that ICT security requirements for the Council are met;
- ensuring the maintenance of all firewalls, secure access servers and similar equipment are in place at all times.

6.6 Head of Service / Team Managers

6.6.1 Heads of Service / Team Managers will take responsibility for ensuring that the Information Management Policy is implemented within their team. All managers will ensure that:

- the requirements of the information management policy framework are met and its supporting policies and guidance are built into local procedures;
- there is compliance with all relevant information management policies within their area of responsibility;
- information management issues are identified and resolved whenever there are changes to services or procedures;
- their staff are properly supported to meet the requirements of information management and security policies and procedures, by ensuring that they are aware of:
  - the policies and procedures that apply to their work area;
  - their responsibility for the information that they use;

- where to get advice on security issues and how to report suspected security incidents.

6.7 Staff

6.7.1 It is the responsibility of each employee to adhere to this policy. Staff will receive instruction and direction regarding the policy from a number of sources, including:

- policy / strategy and procedure manuals;
- their line manager;
- the legal team;
- specific training courses;
- other communication methods, for example, team meetings; and staff intranet.

6.7.2 All staff (whether permanent, temporary, voluntary or on any type of placement / training scheme) and members must make sure that they use the Council's IT systems appropriately and adhere to the relevant ICT Policies of the Council. All members of staff are responsible for:

- ensuring that they comply with all information management policies and information security policies and procedures that are relevant to their service;
- seeking further advice if they are uncertain how to proceed;
- reporting suspected information security incidents.

6.7.3 Staff awareness is a key issue in achieving compliance with Information Management policies. Accordingly there will be:

- mandatory base line training in key information management competencies for all staff;
- additional support for all employees routinely handling 'personal data' as defined by the Data Protection Act 2018;
- all information management policies and procedures available on the intranet;
- staff with specialist knowledge available to advise across the full range of information management areas;
- communication and updates will be provided to staff regularly;
- services are encouraged to have an Information Champion to represent their service. Key messages, training and support are provided to the Information Champions who feed this back to their service. Information Champions can raise issues with the group to identify and remedy problems.

7. MAIN THEMES

7.1 Openness

7.1.1 Non-confidential information which the Council hold will be made available to the public through the Councils website wherever feasible and appropriate.

7.2 Legal Compliance

7.2.1 The main legislation applying to information management is the Data Protection Act 2018 and the Freedom of Information Act 2000. The Council will establish and maintain procedures to ensure compliance with the Data Protection Act 2018, the Freedom of Information Act 2000, the Environmental Information Regulations 2004, and the Humans Rights Act 1998.

7.3 Information Security

7.3.1 Information security is concerned with the confidentiality, integrity, and availability of information in any format, and the Council must comply with the requirements of the Public Services Network.

7.4 Information and Records Management

7.4.1 To ensure that information and records are effectively managed, and that the Council can meet its information management objectives, there will be a Records Management Policy that sets out the Council's standards for handling information during each phase of the information lifecycle.

7.5 Information Quality Assurance

7.5.1 The Council will undertake or commission regular assessments and audits of its information quality and records management arrangements.

7.5.2 Managers are expected to take ownership of, and seek to improve, the quality of data within their services. Training and awareness-raising sessions appropriate to staff groups will be provided.

7.6 Partnerships and Information Sharing

7.6.1 Any sharing of personal or confidential information with partner agencies or involving individual large transfers of such information will be the subject of a written Information Sharing Agreement (ISA). This will set out the expected process, the standards of security and information handling.

8. RISK

8.1 The Council must ensure it operates within a robust information management framework to reduce the risk of threats such as potential litigation, breach of legislation, or enforcement action from the ICO for failure to respond to information requests adequately.

9. TRAINING

9.1 Appropriate training will be mandatory for all staff.

9.2 All staff will be made aware of their obligations for information management through effective communication programmes.

9.3 Each new employee will be made aware of their obligations for information management during an induction-training programme and will be required to undergo mandatory data protection training before they can pass their probation period.

9.4 Training requirements will be reviewed annually to ensure that staff are adequately trained.

10. COMPLIANCE

10.1 Failure to observe the standards set out in this policy may be regarded as serious and any breach may render an employee liable to action under the Council's Disciplinary Procedure, which may include dismissal.

11. FEES AND CHARGES

11.1 The Council aims to provide as much information free of charge on the website for customers to download or view at home. The Council may charge in accordance with the charges set out in legislation or statutory guidance and for the cost of disbursements such as photocopying and postage.

12. COMPLAINTS

12.1 Any person who is unhappy with the way in which the Council has dealt with their request for information, or how their personal data has been handled, may ask for the matter to be reviewed. All complaints should be in writing to:

- DPO@NWLeicestershire.gov.uk (personal data requests)

- FOI@NWLeicestershire.gov.uk (non-personal information request)

- Data Protection Officer
  North West Leicestershire District Council
  Whitwick Road
  Coalville
  Leicestershire
  LE67 3FJ

12.2 Should the requester / complainant still be unhappy with the outcome of this review they have the right to pursue their complaint to the Data Protection Officer for a formal review. Following the Internal Review, the requester can contact the Information Commissioners Office (ICO, www.ico.org.uk) by writing to:

- accessicoinformation@ico.org.uk

- Information Commissioner's Office
  Wycliffe House
  Water Lane
  Wilmslow
  Cheshire
  SK9 5AF

13. EQUALITIES IMPACT ASSESSMENT

13.1 Equality and diversity issues have been considered in respect of this policy and it has been assessed that a full Equality Impact Assessment is not required as there will be no adverse impact on any particular group.

14. REVIEW OF POLICY

14.1 This policy will be reviewed as deemed appropriate, especially in light of any legislative changes, but no less frequently than every 12 months.

14.2 Policy review will be undertaken by the Information Governance Team.

DATA PROTECTION POLICY

Version Awareness

The audience of this document should be aware that a physical copy may not be the latest available version. The latest version, which supersedes all previous versions, is available on our website. Those to whom this policy applies are responsible for familiarising themselves periodically with the latest version and for complying with policy requirements at all times.

Version Control

Version No.	Author	Date Issued	Update Information
V1.0	B Wilson	21.05.2018	Original approved version.
V1.1	N Taylor	28.01.2019	Amended to reflect updated policy.
V1.2	N Taylor	28.05.2020	Updated Sections 4.2, 8.1 and 9.1

May 2020

DATA PROTECTION POLICY

1. INTRODUCTION

Background

1.1 North West Leicestershire District Council (NWLDC) needs to collect person-identifiable information about individuals in order to carry out its functions and fulfil its objectives. Personal data is defined as 'information which relates to a living individual and from which they can be identified, either directly or indirectly'.

1.2 Personal data at NWLDC can include employees (present, past and prospective), service users, contractors and third parties, private and confidential information as well as sensitive information, whether in paper, electronic or other form.

1.3 Irrespective of how information is collected, recorded and processed person-identifiable information must be dealt with properly to ensure compliance with the Data Protection Act 2018 (DPA) and the General Data Protection Regulations 2018 (GDPR).

1.4 The DPA and the GDPR requires NWLDC to comply with the key Data Protection Principles (see Appendix A below) and to notify the Information Commissioner about the data that we hold and why we hold it. This is a formal notification and is renewed annually.

1.5 The DPA and the GDPR gives rights to data subjects (people that we hold information about) to access their own personal information, to have it corrected if wrong, in certain permitted circumstances to ask us to stop using it and to seek damages where we are using it improperly (see Appendix C below).

1.6 The lawful and correct treatment of person-identifiable information by NWLDC is paramount to the success of the organisation and to maintaining the confidence of its service users and employees. This policy will help NWLDC ensure that all person-identifiable information is handled and processed lawfully and correctly.

Data Protection and the GDPR Principles

1.7 NWLDC has a legal obligation to comply with all relevant legislation in respect of data protection and information / IT security. The organisation also has a duty to comply with guidance issued by the Information Commissioners Office.

1.8 All legislation relevant to an individual's right to the confidentiality of their information and the ways in which that can be achieved and maintained are paramount to the Council. Significant penalties can be imposed upon the organisation or its employees for non-compliance.

1.9 The aim of this policy is to outline how the NWLDC meets its legal obligations in safeguarding confidentiality and adheres to information security standards. The obligations within this policy are principally based upon the requirements of the DPA and GDPR, as the key legislative and regulatory provisions governing the security of person-identifiable information.

1.10 Other relevant legislation and guidance referenced and to be read in conjunction with this policy, is outlined together with a brief summary at Appendix B (below).

1.11 GDPR requires Public Authorities to appoint a Data Protection Officer. A Data Protection Officer (DPO) is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). Data Protection Officers are responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements.

2. WHAT INFORMATION IS COVERED

2.1 Personal data within the respective legislative and regulatory provisions covers 'any data that can be used to identify a living individual either directly or indirectly'. Individuals can be identified by various means including but not limited to, their address, telephone number or e-mail address. Anonymised or aggregated data is not regulated by the provisions, providing the anonymisation or aggregation of the data is irreversible.

3. POLICY STATEMENT

3.1 This document defines the data protection policy for NWLDC. It applies to all person-identifiable information obtained and processed by the organisation and its employees.

It sets out:

- the organisation's policy for the protection of all person-identifiable information that is processed;
- the responsibilities (and best practice) for data protection;
- the key principles of the DPA and the GDPR.

4. PRINCIPLES

4.1 The objective of this policy is to ensure the protection of information NWLDC keeps in accordance with relevant legislation, namely:

- **To ensure notification;**

  Annually notified the Information Commissioner about the NWLDC's use of person-identifiable information.

- **To ensure professionalism;**

  All information is obtained, held and processed in a professional manner in accordance with the provisions of the DPA 2018 and the GDPR.

- **To preserve security;**

  All information is obtained, held, disclosed and disposed of in a secure manner.

- **To ensure awareness;**

  Provision of appropriate training and promote awareness to inform all employees of their responsibilities.

- **Data Subject Access;**

  Prompt and informed responses to subject access requests.

4.2 The policy will be reviewed periodically by the NWLDC Information Governance Team. Where review and update is necessary due to legislative changes this will be done immediately.

4.3 In accordance with the council's equality and diversity policy statement, this procedure will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, union membership, disability, offending background or any other personal characteristic.

5. SCOPE OF THIS POLICY

5.1 This policy will ensure that person-identifiable information is processed, handled, transferred, disclosed and disposed of lawfully. Person-identifiable information should be handled in the most secure manner by authorised staff only, on a need to know basis.

5.2 The procedures cover all person identifiable information, electronic or paper which may relate to employees, contractors and third parties about whom we hold information.

6. POLICY

6.1 NWLDC obtains and processes person-identifiable information for a variety of different purposes, including but not limited to:

- staff records and administrative records;
- Service Users records including the administering of benefits, council tax, housing records, elections, grants, planning applications, licensing applications, etc;
- matters relating to the prevention, detection and investigation of offences, fraud and corruption;
- matters relating to the enforcement of primary and secondary legislation;
- complaints and requests for information.

6.2 Such information may be kept in either computer or manual records. In processing such personal data, NWLDC will comply with the data protection principles within the DPA and GDPR.

7. DATA PROTECTION RESPONSIBILITIES

Overall Responsibilities

7.1 The Council is the 'data controller' and permits the organisation's staff to use computers and relevant filing systems (manual records) in connection with their duties. The Council has legal responsibility for the notification process and compliance with the DPA and the GDPR.

7.2 The Council whilst retaining its legal responsibilities has delegated data protection compliance to the Data Protection Officer.

Data Protection Officer's (DPO) Responsibilities

7.3 The Data Protection Officer's responsibilities include:

- ensuring that the policy is produced and kept up to date.
- Ensuring that the appropriate practice and procedures are adopted and followed by the Council.
- Provide advice and support to the Senior Management Team on data protection issues within the organisation.
- Work collaboratively with Human Resources, the Head of Law and Governance and the Compliance Team to help set the standard of data protection training for staff.
- Ensure data protection notification with the Information Commissioner's Office is reviewed, maintained and renewed annually for all use of person identifiable information.
- Ensure compliance with individual rights, including subject access requests.
- Act as a central point of contact on data protection issues within the organisation.
- Implement an effective framework for the management of data protection.
- Review Retention Schedule annually in January to ensure that it is accurate and up to date.
- Conduct department reviews to ensure that all departments are compliant and act in accordance with the retention schedule.

Line Managers' Responsibilities

7.4 All line managers across the Council's service areas are directly responsible for:

- ensuring their staff are made aware of this policy and any notices;
- ensuring their staff are aware of their data protection responsibilities;
- ensuring their staff receive suitable data protection training.

General Responsibilities

7.5 All NWLDC employees, including temporary and contract staff are subject to compliance with this policy. Under the GDPR individuals can be held personally liable for data protection breaches.

7.6 All NWLDC employees have a responsibility to inform their line manager and the Data Protection Officer of any new use of personal data, as soon as reasonably practicable after it has been identified.

7.7 All NWLDC employees will, on receipt of a request from an individual for information held, known as a subject access request or concerns about the processing of personal information, immediately notify the Compliance Officer.

7.8 Employees must follow the subject access request procedure (see Appendix C below).

8. MONITORING

8.1 Compliance with this policy will be monitored by the Corporate Leadership Team, together with internal audit reviews where necessary.

8.2 The Data Protection Officer is responsible for the monitoring, revision and updating of this policy document on an annual basis or sooner, should the need arise.

9. VALIDITY OF THIS POLICY

9.1 This policy will be reviewed at least annually by the Information Governance Team. Associated data protection standards will be subject to an ongoing development and review programme.

APPENDIX A

GENERAL DATA PROTECTION REGULATION 2018 - THE DATA PROTECTION PRINCIPLES

1. Lawfulness, Fairness and Transparency: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

2. Purpose Limitation: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

3. Data Minimisation: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Accuracy: Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. Storage Limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

6. Integrity and Confidentiality: Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7. Accountability: The controller shall be responsible for, and be able to demonstrate compliance with, the previous six principles.

APPENDIX B

SUMMARY OF RELEVANT LEGISLATON AND GUIDANCE

General Data Protection Regulations (GDPR)

A legal basis must be identified and documented before personal data can be processed. 'Controllers' and 'Processors' will be required to document decisions and maintain records of processing activities.

Human Rights Act 1998

This Act binds public authorities to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and a service user's right to expect confidentiality of their information at all times.

Article 8 of the Act provides that "everyone has the right to respect for his private and family life, his home and his correspondence". However, this article also states "there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

Freedom of Information Act 2000

This Act gives individuals rights of access to information held by public authorities.

Regulation of Investigatory Powers Act 2000

This Act combines rules relating to access to protected electronic information as well as revising the "Interception of Communications Act 1985". The aim of the Act was to modernise the legal regulation of interception of communications, in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998

This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area. The Act allows disclosure of person-identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose person identifiable information and responsibility for disclosure rests with the organisation holding the information.

The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. NWLDC issues each employee with an individual user id and password, which will only be known to the individual and must not be divulged to other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act. NWLDC will adhere to the requirements of the Computer Misuse Act 1990, by ensuring that its staff are aware of their responsibilities regarding the misuse of

computers for fraudulent activities or other personal gain. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

This Act allows employers to intercept and record communications in certain prescribed circumstances for legitimate monitoring, without obtaining the consent of the parties to the communication.

APPENDIX C

INDIVIDUAL RIGHTS OF THE DATA SUBJECT

1. The Right to be Informed: Individuals have the right to be provided with clear and concise information about what an organisation does with their personal data. NWLDC has published Privacy Notices for each of its departments that outline in detail what data we collect, how that data is used, the lawful basis for processing the data and for how long we will retain that data. These can be found on our website at:

   https://www.nwleics.gov.uk/pages/data_protection_notice

2. The Right of Access: Individuals have the right to access their personal data that is held by an organisation (commonly referred to as Subject Access). You have the right to obtain a copy of your personal data by making a Subject Access Request as detailed below.

3. The Right to Rectification: Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete. You can make a request for rectification as detailed below.

4. The Right to Erasure: Individuals have the right to have their personal data erased or 'forgotten' in certain circumstances. These include when the data is no longer necessary for the purpose in which we originally collected or processed it, when we are relying on your consent to process the data and you choose to withdraw that consent, when we are relying on legitimate interests as our basis for processing and you object to this processing (so long as there is no overriding legitimate interest to continue this processing), we have processed the personal data unlawfully, we have to do it to comply with a legal obligation or we have processed the personal data to offer information society services to a child. The Right to Erasure is not an absolute right and only applies in these circumstances listed; however, we will make every effort to assist you. You can make a request for erasure as detailed below.

5. The Right to Restrict Processing: Individuals have the right to restrict or suppress the processing of their personal data where they have a particular reason for wanting the restriction. This is not an absolute right and only applies in certain circumstances. When processing is restricted, we are permitted to store the data, but not to use it. This right may apply if you are contesting the accuracy of your data and we are verifying that accuracy, if the data has been unlawfully processed and rather than invoking the Right to Erasure you request restriction instead, if we no longer need the personal data but you need NWLDC to keep it in order to establish, exercise or defend a legal claim, or you object to our processing of your data and we are considering whether our legitimate grounds for processing override your request. You can request the restriction of data processing as detailed below.

6. The Right to Data Portability: Individuals have the right to obtain and reuse their personal data for their own purposes across different services. This allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. You have the right to request that we transfer the data you have provided to NWLDC directly to another Data Controller. This right only applies when the lawful basis for processing the information is consent or for the performance of a contract and we are carrying out the processing by automated means (in other words, it excludes paper files). You can make a data portability request as detailed below.

7. The Right to Object: Individuals have the right to object to the processing of their data in certain circumstances. You have the absolute right to stop your data being used for direct marketing. You may also object to processing if it is for a task carried out in the public interest, the exercise of official authority vested in us or our legitimate interests (or those of a third party); however, the right to object is not absolute in these circumstances. You can make an objection as detailed below.

8. Rights in Relation to Automated Decision Making and Profiling: The GDPR has provisions on making a decision solely by automated means without any human involvement and the automated processing of personal data to evaluate certain things about an individual. All automated decision-making and profiling is subject to the GDPR and NWLDC will identify, when applicable, whether any of our data processing relies solely on automated decision-making or whether we use profiling of any kind. This information is available on our website at:

   https://www.nwleics.gov.uk/pages/data_protection_notice

To invoke these rights, simply submit your request to us in writing either by email at dpo@nwleicestershire.gov.uk or to:

North West Leicestershire District Council
Council Offices
Whitwick Road
Coalville
Leicestershire
LE67 3FJ

For all requests, NWLDC will have one calendar month in which to respond.

Document Control

Prepared By	Data Protection Officer
Original Authorisation By	Senior Management
Review Period	One year
Classification	Public

This page is intentionally left blank

ICT AND CYBER SECURITY POLICY

Version Control

Version No.	Author	Date	Update Information
2.3	Sam Outama	22.06.2020	General review and update
2.2	Sam Outama	30.05.2019	Update to Cyber Security
2.1	Sam Outama	14.09.2017	Update Password Control
2	Sam Outama	25.07.2017	General Update
1.1	Ivan Arkinstall	09.07.2013	Revised
1	Phil Clarke	04.03.2009	Revised

June 2020

ICT AND CYBER SECURITY POLICY

FORWARD

North West Leicestershire District Council is dependent upon its Information and Communications Technology (ICT) systems for its normal day to day business activities. It is therefore essential for the continued successful operation of the Council that the confidentiality, integrity and availability of its ICT systems and data are maintained at a high level at all times. There is also an obligation on the Council and all employees to comply with relevant legislation such as the General Data Protection (GDPR) Acts, the Copyright, Designs and Patents Act and the Misuse of Computers Act.

The majority of information used by the Council is now available and kept in an electronic format and this policy is centred on the need to ensure that our technology and IT systems are sufficiently secure to protect the underlying information and suitably protected. This does, however, need to be backed by a wider culture of confidentiality and security of information in any form including direct conversations, telephone conversations and the written word.

It follows that the highest standard of IT security is required within the Council. To achieve this, the ICT Security and Cyber Security Policy has been introduced and everyone who uses IT equipment is expected to read it and ensure that its provisions are complied with. There is also a short summary of this policy containing the main aspects affecting the average user.

The key to ensuring that the Council's data and systems remain secure is to ensure that all staff are aware of their own responsibilities they will be required to:

- acknowledge receipt and understanding of this policy document;
- in the case of staff having access to RESTRICTED data via the Government Connect Secure Extranet (GCSx) or Government Secure Intranet (GSi) will agree to abide by specific ICT security rules regarding such information (see Appendix 2).

Wilful failure to follow the procedures stated in this policy may lead to disciplinary action, prosecution and may also render the person personally liable for the cost of replacing or reinstating damaged or corrupt equipment and data.

The policy will be reviewed periodically (at least annually) and updated by the ICT Manager. If you have any doubts about the meaning of any part of this policy, or believe that it could be improved in any way, please contact the ICT Manager.

POLICY OBJECTIVES

This policy also sets out the overall objective and principles underlying ICT and cyber security at North West Leicestershire District Council and specifies the management arrangements and key responsibilities.

The objective of this ICT and Cyber Security Policy and its supporting policies is to ensure the highest standards are maintained across the Council at all times so that:

(a) the public and all users of the Council's information are confident of the confidentiality, integrity and availability of the information used and produced.

(b) Business damage and interruption caused by cyber security incidents are minimised.

(c) All legislative and regulatory requirements are met.

(d) The Council's information is used responsibly, securely and with integrity at all times and that this applies to manual and electronic information.

The main objectives of this policy are:

- to ensure adequate protection of all the Council's assets, locations, people, programs, data and equipment, on a cost-effective basis, against any threat which may affect their security, integrity and/or the level of IT service required by the Council to conduct its business;
- to ensure awareness amongst the Council's officers and members of all relevant legislation and that they fully comply with such legislation;
- to ensure awareness within the Council of the need for IT and cyber security to be an integral part of the day to day operation of the Council's business;
- to ensure user security awareness training is in place and all staff have access to that training.

The strategic approach to cyber security is based on:

- consistency of approach with the implementation of key processes and procedures
- the application of recognised security management good practice such as the Cyber Essentials PLUS and ISO/IEC 27000 family of information management systems standards;
- implementation of physical, personal, procedural and technical counter and mitigation measures;
- annual cyber security assessments and risk mitigations of external and internal threats, commonly called ICT security penetration test carried out by a third party CREST/IASME accredited supplier;
- the continuing availability of specialist security advice;
- cyber security is a vital area of concern, with ever increasing threat vector, that will receive the regular attention of senior management, through the risk and management committee and the Corporate Leadership team;
- all users have an essential role to play in maintaining sound IT and cyber security and will be fully supported by attending QTRLY user awareness security training;
- yearly IT audits conducted by an external supplier, to provide assurance on key ICT controls.

SCOPE

This Information Technology and Cyber Security Policy will apply to:

- all the Council's employees, members, contractors, partners and agents;
- all assets owned by the Council;
- information held or owned by North West Leicestershire District Council, any ICT equipment and infrastructure used, and the physical environment in which the information and/or supporting ICT is used;
- all members of the Council who use the Council's ICT facilities;
- employees and agents of other organisations who directly or indirectly support the Council's IT services;
- members of the public using IT resources to access data on Council premises;
- Council's systems in a hosted / cloud environment.

Where access is to be granted to any third party (e.g. contractors, service providers, voluntary agencies, and partners) compliance with this policy must be agreed and documented, following the third party code of connections policy in Appendix 3. A copy of this policy and the summary document will be issued to all the above.

1. SECURITY ORGANISATION

Objective:

To manage information and cyber security within North West Leicestershire District Council to the highest level.

1.1 Responsibilities

The ICT Manager is responsible for:

- assigning security roles and responsibilities;
- co-ordinating the implementation of the security policy across the Council;
- reviewing and if appropriate updating the Security Policy;
- reviewing and monitoring security incidents;
- reviewing third party access and security arrangements;
- monitoring exposure to major threats to information assets;
- agreeing and supporting Council-wide security initiatives;
- ensuring patch management of devices is performed on a monthly basis and monitored.

The security of all hardware situated in departments and sections is the responsibility of the departmental or service manager.

The security of all other hardware, operating systems, PC application, networking, infrastructure and corporate software is the responsibility of the ICT Manager.

Departmental application software is the responsibility of:

Application	**System Administrator**	**System and Data Owner**
General Ledger	Financial Planning	Head of Finance
Creditors and Debtors	Exchequer Services	Head of Finance
Payroll	HR	Head of HR and Organisation Development
Revenues and Benefits	Partnership	Head of Customer Services
Housing Management	Strategic Housing	Head of Housing
Housing repairs	Strategic Housing	Head of Housing
Cash Receipting	Exchequer services	Head of Finance
Planning, Building Control	ICT	Head of Planning and Regeneration

Geographic Information System	ICT	Head of Planning and Regeneration
Environmental Health and Licensing	ICT	Head of Community Services
Electoral Registration and Elections	Elections Officer	Head of Legal and Commercial Services
Personnel	HR and Organisation Development	Head of HR and Organisation Development
Land Charges	ICT	Head of Planning Services and Regeneration
Electronic Document Management	ICT	Head of Planning services and Regeneration
Leisure Services Bookings	Business Development manager (Leisure)	Head of Community Services

1.2 Acquisition of Information and Communications Technology

All acquisitions of Information and Communications Technology (ICT) shall be in accordance with Council Procurement Procedures and be co-ordinated by the ICT Manager who shall obtain specialist advice if he considers it appropriate.

All new acquisitions of a corporate nature shall be agreed by the Corporate Leadership Team.

Departmental acquisitions shall be agreed between the appropriate Head of Service and the ICT Manager.

The ICT Manager has delegated authority to replace obsolete equipment in accordance with an agreed replacement program and to upgrade/replace office productivity tools and software within an agreed programme.

All new projects will be in accordance with the Council's corporate project management policies, have associated business case / justification documents and be in accordance with the current ICT strategy / road map.

1.3 Security Information Advice

Specialist advice on information security is available internally from the ICT Manager or Internal Audit.

1.4 Security Incidents

All suspected and actual security incidents shall be reported immediately to the ICT Service desk. Each incident will be recorded, investigated and corrective action implemented where appropriate. If the incident is perceived to be of a serious or urgent nature it will be escalated to the ICT manager or the Head of Customer Services.

The Council has a separate ICT Security Incident Reporting Procedure which gives full details on how to report any security incidents and this includes a copy of the reporting form which you may be asked to complete by the ICT Service desk.

This document is available from within the IT section of the Council Intranet

1.5 Independent Review of Information Security

The content, implementation and practice of this policy will be reviewed independently to provide assurance that organisation practices properly reflect the policy and that the policy is feasible and effective. Independent reviews will be carried out by the internal Audit team and External Auditors (KPMG) or one that has been appointed.

2. SECURITY OF THIRD PARTY ACCESS

Objective:

To maintain the security of organisational ICT facilities and information assets accessed by third parties. Either on premise or hosted environment.

2.1 Identification of Risks from Third Party Connections

Where there is a business need for third party access to ICT facilities and information assets the security implications and requirements will be determined, and controls agreed with the third party.

All new systems will be assessed for risks from third party connections and, where appropriate, controls will be defined in a contract with the third party, as described in Appendix 3.

Arrangements involving third party access, e.g. Support engineers, subcontractors, consultants will be based on a formal contract or security agreement containing, or referring to, all of the necessary security conditions to ensure compliance with the Council's security policy including obtaining an indemnity in respect of any loss caused by erasure or alteration of data or incorrect alteration of programs. The contract should be in place before access to the ICT facilities is provided.

See Appendix 3 for sample security agreement for use by third parties.

The implementation of any changes to systems should be strictly controlled using formal change control procedures. Any third party organisation carrying out work for the Council will be expected to comply with these change control procedures and will ensure that all system changes are documented. The ICT change control policy is available via the ICT intranet page.

All third party access will be controlled and is available to service providers via a secure internet connection using an SSL (secured sockets layer) VPN appliance, or an application such as Team Viewer.

Where reasonably possible, for all access will use multi factor authentication using a soft token delivered via SMS to the user's mobile phone or a mobile app. The remote support user will be given an access code and a onetime use password for that session.

All systems have passwords enabled to ensure only authorised parties can access the Council's ICT, at agreed times and that each third party can only access the relevant systems.

All contractors, consultants or other temporary staff will be issued with a unique user code and password in line with current procedures for the particular system being used. **Under no circumstances should Council staff allow their own user code or password to be used by anyone else**.

In certain circumstances it may be necessary to divulge a password for access by technical support staff and in such cases, it must be changed immediately after the authorised activities are completed. A log of such activity is maintained by the ICT department.

A log of all third party access will be recorded on the Service Desk management system, with a copy of the completed third party access control form. All third parties accessing Council systems or data must have had their own IT Security tested by a trusted third party or hold a valid accreditation such as Cyber Essentials or ISO 27001.

3. ASSETS CONTROL

Objective:

To maintain appropriate protection of organisational assets:

3.1 Inventory of Assets

An inventory of ICT assets shall be maintained by the ICT Manager who shall promptly update it for all acquisitions, disposals, updates and management of our cyber assets (this include transfer of assets to another user).The accuracy of the inventory shall be verified annually in accordance with Financial Procedure Rules. This includes equipment at staff homes for those who are working in an agile manner.

All users must notify ICT if they move an asset to another location, within the Council Offices or a remote site.

4. PERSONNEL SECURITY

Objective:

To reduce the risks of human error, theft, fraud or misuse of facilities:

4.1 General

Security roles and responsibilities for all staff using ICT facilities will be included in job descriptions and contracts where appropriate by the relevant manager. Managers are responsible for ensuring job descriptions or codes of conduct address all relevant security responsibilities.

All potential recruits will be screened by:

- obtaining two satisfactory references;
- confirming academic and professional qualifications.

All employees and third party users of ICT facilities will be required to sign a confidentiality (non-disclosure) undertaking. Revenue Services benefits staff will be subject to recruitment procedures included in the Benefits Anti-Fraud Strategy.

The appointment of employees with access to information classified as PROTECT or RESTRICTED (see Appendix 1) will be subject to the specific Baseline Personnel Security Standards available on request from the Human Resources department.

All users are responsible for the equipment issued to them and information that they have access to. Third party access to ICT equipment and data, without prior arrangement with IT is prohibited. When accessing Council information, they must ensure that they do so in a secure environment and that persons who are not authorised to view said information cannot view it.

4.2 ICT and Cyber Security Training

Objective:

To ensure that users are aware of information security and cyber threats and concerns, and are equipped to comply with and support the Council's security policy in the course of their work:

All users will need to undertake a cyber security user awareness e-learning training module.

All ICT users will be briefed in security procedures and the correct use of ICT facilities by IT staff in order to minimise possible security risks to the confidentiality, integrity and availability of data or services through user error. Managers are responsible for ensuring such training is provided to their staff.

New user accounts will only be established and issued to staff who have received appropriate ICT induction and have been authorised by the relevant Head of Service or Director. All new ICT users will be issued with either a paper copy of the current ICT and Cyber Security Policy or given access to the document on the Council's intranet. They must read the document and sign to acknowledgement the terms and conditions within 2 working weeks otherwise network access will be denied.

All new ICT users who will have access to the Government Connect Secure Extranet (GCSx) or Government Secure Internet (GSi) networks will be also be required to comply with a Personal Commitment Statement pertaining to those services.

Access levels to review / amend / delete data will be determined by the relevant Head of Service in association with the system owner(s) of any ICT applications which the new user intends to use.

All third party suppliers, contractors and temporary staff will be required to read and acknowledge the terms and conditions before being granted access to Council ICT resources.

In the case of third party support companies where individual users may not be easily identifiable a board level representative of the company will be required to acknowledge the terms and conditions.

4.3 Responding to Incidents

Objective:

To minimise the damage from security incidents and malfunctions, and to monitor, learn from and reinforce procedures in the light of such incidents:

A security incident shall mean:

- any event arising from negligence or deliberate default that has, or could have, resulted in loss or damage to the Council's IT systems or data;
- a compromise to the confidentiality, integrity or availability of IT systems or data;
- an action that is in breach of the security policy;
- any cyber security threat or incident.

All security incidents shall be reported immediately to the ICT Service Desk who will pass the calls to the ICT Security Officer or ICT Manager who will instigate an investigation and report any incidents that cause serious loss or damage to the Head of Customer services and the Data protection officer. Any security incident that may have the potential to lead to disciplinary action will involve the appropriate involvement and consultation with the Head of Human Resources and Organisation Development and/or (depending upon the nature of the incident) the Audit Services Manager.

The Council has a separate ICT Security Incident Reporting Procedure which gives full details on how to report any incidents and this includes a copy of the reporting form which you may be asked to complete by the ICT Service desk. This document is available from within the IT section of the Council Intranet. The security incident will also be logged on the ICT Service Desk system.

Any security incident which leads to loss or damage, or wilful abuse of the conditions of this policy may be cause for investigation and, where appropriate, formal action, in accordance with the Council's agreed disciplinary policy.

Any incident or suspected incident must be handled in the manner as laid out in the Council's Incident and Response Policy and Procedures. The above Incident Response Policy and Procedures will be reviewed on a yearly basis.

5. PHYSICAL AND ENVIRONMENTAL SECURITY

Objective:

To prevent unauthorised access, damage and interference to ICT services to prevent loss, damage or compromise to assets and to the confidentiality, integrity or availability of IT systems or data, and interruption to business activities:

5.1 Secure Areas

ICT facilities such as servers, server rooms and hosting facilities, hubs and routers supporting critical or sensitive business activities shall be housed in secure areas, i.e. protected from unauthorised access, damage and interference.

Except for systems specifically intended for public use, ICT facilities should only be available to authorised persons, and wherever possible should be kept away from

public access, and preferably view. Specialised IT equipment should be further restricted to authorised staff only in areas of extra security.

The following specific conditions will apply to such secure areas:

- server rooms will be protected by electronic locking systems or digital locks on all entry points and will always be kept locked;
- access to any hosted / Data Centre facility is only for NWLDC ICT staff, with proof of identification and access granted via a request system or logging portal;
- access to server rooms will be only to ICT support staff or to others acting under their close supervision;
- server rooms will be protected with fire detection and control equipment (FM200 Gas). Such equipment will be integrated into the Council's overall fire detection system;
- servers will be protected by Uninterruptible Power Supplies (UPS) enough to allow continuous working of equipment for a minimum of 2 hours in the event of loss of electrical supply to the rooms;
- server rooms will be regularly monitored to ensure an adequate operating environment for the equipment contained;
- network distribution cabinets will be protected with UPS enough to allow continuous working for a minimum of one hour;
- network distribution cabinets will always be kept locked and access granted only to ICT network support staff or others acting under their close supervision;
- remote access may be allowed to server, network and telephony equipment but will be limited to ICT support staff and specified third party support organisations. (Access by third parties will be subject to agreements specific to the software / equipment concerned and, always, will be with the express permission of ICT staff). This includes completing the Permit to work and Risk assessment documents, for all external contractors requiring access to the server room;
- A complete log of remote access by third party support organisations will be maintained.

5.2 Equipment Security

ICT equipment and cabling should be protected from spillage or leaks and must be sited away from where staff or the public walk and also to minimise opportunities for unauthorised access or removal. Staff should also be warned of the dangers of spilling liquids or food on IT equipment. **Except for laptop and portable computers only IT staff should move, or supervise the moving, of IT equipment**.

All critical ICT equipment shall be protected by an uninterruptible power supply (UPS). UPS equipment should be self-testing and shall also be manually tested by IT staff at least every six weeks and serviced as necessary.

Officers and members should always ensure that computer equipment and screens are positioned to prevent unauthorised viewing of data.

Any faulty ICT equipment shall be reported to the IT section who will arrange for its repair or replacement. **Under no circumstances shall members of staff attempt to repair, move, change equipment or open casings except for printers to replace consumables or clear a paper jam**.

Computers provided by the Council for use at home are for the sole use of that officer or member, no unauthorised third party is allowed access to the computer equipment

for any reason. **The officer or member will be responsible for ensuring that computer is, always, used in accordance with Council conditions of use**.

Laptop, portable computers and smart phones (unless permanently assigned to an officer or member) may be borrowed, with the permission of the officer's manager, from the IT section who will maintain a record of issue and returns. Such equipment must be transported in appropriate carrying cases, must not be left in clear view in a vehicle or left in an unattended or unlocked vehicle when other, more secure, accommodation is available. **Officers should treat laptop, smart phones and portable computers as if it were their own possession and uninsured**.

Any laptops, smart phones or computers currently assigned on a permanent basis to an officer or member can be recalled for a software audit on a one-week notice. The officer or member must arrange a mutually convenient time when the computer can be returned to the IT department within that week period. Once the audit has been conducted the IT department will either return the computer or inform the officer or member and arrange a collection time and date.

5.3 Equipment and Data Destruction

Obsolete equipment shall be checked by IT staff and all hard disks will be thoroughly cleansed of data before disposal, whether by sale, donation or destruction. Equipment will normally be disposed of via a third party accredited data disposal organisation who will ensure recycling, where possible. Any PCs disposed of by sale / donation will not include the operating system installed and no application software.

All ICT equipment will be disposed of in accordance with the relevant environmental legislation e.g. WEEE Directives.

A separate procedure document "Managing, Tracking and disposing of ICT assets", is available on the ICT intranet page.

5.4 Remote Access to Systems and Data

Where there is a business need, the Council will allow employees and members to have remote access to data and systems from locations not covered by the Council local and wide area networks. This will include 'roaming' users who with suitable technology are able to access data anywhere and 'fixed point' users such as home workers. Access to systems from non-council devices, will be controlled via multi factor authentication.

The Council will allow such remote users to make use of their own PC equipment subject to meeting minimum security standards including having up to date anti-virus and firewall software.

Remote access to Council systems will only be granted on the Authority of the relevant Head of Service or Director

Remote access will be only available by using multi factor authentication (i.e. the use of a 2 part password). NWLDC operates soft tokens which require the use of a unique personal PIN either sent to the work mobile combination with a dynamically generated pass code or generated with a mobile app.

Specific conditions and responsibilities will apply to those users:

- data must not be stored on non-Council devices used for remote access;
- confidential data must be encrypted on storage devices supplied by the ICT department;
- particular care should be taken with removable storage devices such as USB sticks, etc and if these are used to move or transfer data it must be stored in encrypted format using supplied “Safe Sticks”;
- any Council data downloaded or stored on employees’ remote users’ PC equipment must be kept secure and inaccessible to others. Data must be removed as soon as is practicable when it is no longer required;
- any loss of equipment (own or Council) must be reported immediately to the ICT Service Desk;
- any actual or perceived security threat relating to remote use of Council IT systems must be reported immediately to the ICT Service Desk;
- no RESTRICTED information should ever be used on employees / members own equipment.

When undertaking video or conference calls discussing or displaying Council information, they must ensure that no unauthorised person are privy to that information.

6. COMPUTER AND NETWORK MANAGEMENT

6.1 Operational Procedures and Responsibilities

Objective:

To ensure the correct and secure operation of computer and network facilities:

The ICT Manager is responsible for the management and operation of all servers and networks and associated specialised hardware. Departmental managers are responsible for the safe day to day operation of portable and desktop computers and printers issued to them or their staff.

Appropriate documented procedures for the management and operation of all servers and networks will be established by computer staff.

Clearly documented procedures shall be prepared by computer staff and/or the system administrator for all operational computer systems to ensure their correct, secure operation.

6.2 System Planning and Acceptance

Objective:

To minimise the risk of systems failure:

Advance planning and preparation are required to ensure the availability of adequate capacity and resources.

Acceptance procedures for new systems will include the following:

- performance and computer capacity;
- preparation of error recovery and restart procedures;
- preparation and testing of routine operating procedures;

- evidence that the new system will not adversely affect existing systems, particularly at peak processing times;
- training in the operation or use of new systems;
- formal consideration of the need for ongoing maintenance and support by a third party.

Emergency fall back arrangements should be identified for each system and adequate fall-back arrangements made wherever possible. Fall back arrangements for each system should be fully documented and responsibility for this lies with the relevant system administrator.

6.3 Configuration and Change Management

Objective:

To document and manage the ICT structure and any changes thereto:

Operational changes must be controlled to reduce the risk of system or security failures. The ICT Manager is responsible for ensuring that changes to software or hardware are carried out in a controlled manner and appropriately documented.

A formal change control (and authorisation) is in place which requires significant changes to software and hardware to be assessed, tested and verified before completion. This procedure will apply to anyone making such changes including permanent staff, temporary and contract staff, suppliers and third party support organisations.

All PCs and servers are configured and installed with a standard security configuration, which may be changed only on the authority of the ICT Manager. Any attempts to amend the standard configuration will be logged and monitored.

Specific protective measures are applied to servers accessed by users outside the Council's main network. Such servers are in a separate secure zone of the network known as a de-militarised zone or DMZ.

Please refer to "ICT Server Build Policy" and "ICT PC Build Policy" for full details.

Changes to software and hardware will, wherever possible, be applied in a test environment before being applied to operational systems.

6.4 Protection from Malicious and Unauthorised Software

Objective:

To safeguard the integrity of software and data:

It is essential that special measures, as detailed below, are implemented to prevent the introduction of malicious software such as computer viruses, ransomware and malware or the use of unauthorised software. Using unlicensed software can result in a raid (authorised by the courts) to identify the use of such unlicensed software which can result in a fine, adverse publicity and a block on the use of ANY computers until the licences are paid for or the offending software is removed, resulting in very serious disruption to the organisation's activities.

In extreme cases staff could face imprisonment. A computer virus or similar can cause severe damage to data and hence serious disruption. Every precaution must be taken to protect Council data and programs.

Unauthorised software is software that has not been purchased by, or whose purchase or use has not been agreed by the ICT Manager.

To reduce the risks of infection or use of unauthorised software the following preventive, detective and corrective measures will be instituted:

- **the introduction and/or use of unauthorised software, including screensavers, is prohibited and may lead to the application of relevant, formal disciplinary action;**
- software licences will be complied with at all times;
- Reputable, up to date anti-virus software will be used to detect and remove or isolate viruses and malware;
- **staff or members must not transfer data from their home PC to the Council computers, whether by removable storage media or e-mail, unless their home PC has up to date (i.e. definitions updated within the previous week) anti-virus software and firewall installed. The anti-virus software used must be one verified by the Council's ICT support staff;**
- **removable storage media devices are blocked from being connected to corporate devices;**
- any suspected viruses must be reported immediately to the computer section and, where appropriate, logged as a security incident;
- except where there is a justifiable business reason that has been expressly agreed with the ICT Manager, users should not open unsolicited e-mails from unverifiable sources and especially any attachments as there is a significant risk, they may contain a virus;
- **users must not attempt to download executable files, i.e. program software, from the Internet without prior specific clearance from IT staff;**
- any incoming e-mail that contains executable or compressed attachments will be automatically quarantined and routed to IT staff for checking before delivery to the intended recipient.

USB devices and removable media are not allowed on any machine. Device management software is in place to detect and block this type of activity. ICT can provide encrypted USB "safe sticks" for transfer of data, which is prohibited on all machines.

6.5 Housekeeping

Objective:

To maintain the integrity and availability of IT services:

Housekeeping measures are required to maintain the integrity and availability of services.

Routine procedures will be established by computer staff for taking back-up copies of data, logging events and, where appropriate, monitoring the equipment environment.

Documented procedures for each system shall include:

- data back-up,
- operator logs,
- fault logging,
- environmental monitoring,
- network and application restart procedures,
- change request logs,
- system updates / upgrades.

6.6 Network Management

Objective:

To ensure the safeguarding of information in networks and the protection of the supporting infrastructure:

Appropriate controls must be implemented to ensure the security of data in networks and the protection of connected services from unauthorised access.

Each authorised user will be allocated a unique logon identifier by ICT Support staff and a password that the user must change at least every 90 days. The password must contain at least eight characters including a mixture of three of the following four elements (a complex password):

- lower case alpha characters,
- upper case alpha characters,
- numbers,
- special characters.

The password policy is to be reviewed on a yearly basis following guidance issued by NCSC.

Access to the network is automatically barred after four successive unsuccessful attempts to logon. Users are responsible for ensuring the secrecy and quality of their password and shall be held responsible for all actions recorded against their unique logon identifier.

The ICT Manager is responsible for ensuring the security of the networks.

A separate procedure document is available “Starters and Leavers Process Including Domain Account Administration” on the ICT intranet page.

6.7 Media Handling and Security

Objective:

To prevent damage to assets and interruptions to business activities:

Computer media containing data shall be controlled and physically protected.

Appropriate operating procedures will be established to protect computer media (tapes, disks, cassettes) input / output data and system documentation from damage, theft and unauthorised access.

At least one copy of all computer media containing data or critical software will be stored in media fire safes. A copy of all such media should also be kept securely offsite.

Computers that rarely physically connect to the network such as laptops or computers provided to members and some officers are not covered under our backup policy and data backups of these computers is the responsibility of the member or officer. A means of backing up the computer and a lesson on how to backup data will be provided by the ICT department

6.8 Data and Software Exchange

Objective:

To prevent loss, modification or misuse of data:

Exchanges of data or software between the Council and third parties should be managed in accordance with the data classification table in Appendix 1.

For critical or sensitive data and software, formal agreements, (including software escrow agreements where appropriate) for exchange of data and software (whether electronic or manual) between organisations should be established. These agreements should specify appropriate security conditions which reflect the sensitivity of the information involved, including:

- management responsibilities for controlling and notifying transmission, despatch and receipt,
- minimum technical standards for packaging and transmission,
- courier identification standards,
- responsibilities and liabilities in the event of loss of data,
- data and software ownership and responsibilities for data protection, software copyright compliance and similar considerations,
- technical standards for recording and reading data and software,
- any special measures required to protect very sensitive items
- The use of personal e-mails for sharing of data is prohibited

In order to ensure security of physical media in transit reliable transport couriers should always be used. Packaging should be sufficient to protect the contents from any physical damage during transit and should be in accordance with manufacturers' instructions.

Data in transit should be sealed with tamper proof or evidence devices and have accompanying documentation to list package contents.

All electronic commerce should be in accordance with the Council's Contract Procedure Rules / Financial Procedure Rules and subject to formal contract(s) drawn up between the Council and the trading partner(s), including the specialised areas of communication processes, transaction message security and data storage. Managers will need to obtain the appropriate specialised advice upon, identify and take into account all external and internal requirements affecting this activity. These requirements are likely to include the acts and directives listed in section 9.1 of this policy. Also relevant will be international and local (to other countries) laws and directives, any national or international professional regulations such as accounting practice and tax regimes, any conditions specified by the Council's insurers, fair trade and human rights standards, and the requisite information and technology standards

and controls to preserve the timeliness, accuracy and integrity, security, recoverability and processing of this activity.

6.9 Connection to Other Networks

Objective:

To facilitate use of this means of communication while preventing risks to the Council from inappropriate use:

For operational purposes, the Council will sometimes require access to external networks both to make use of business applications and to exchange data. Access to such networks is only allowed under the following conditions:

- must be authorised by the relevant Head of Service;
- must be agreed by the ICT manager or ICT Security Officer;
- must be protected by a firewall configured to provide protection of all networks concerned;
- must be subject to a suitable data sharing agreement / contract;
- must have protocols in place to protect data in transit and at rest.

6.10 Electronic Mail

Objective:

To facilitate use of this means of communication while preventing risks to the Council from inappropriate use:

Controls to reduce the security risks associated with electronic mail (e-mail) should be implemented covering:

- vulnerability to unauthorised interception or modification. Confidential data should only be sent in encrypted form;
- vulnerability to error, for example incorrect addressing;
- legal considerations such as the need for proof of origin, despatch, delivery and acceptance;
- publication of directory entries;
- remote access to e-mail accounts.

All staff have internal e-mail facilities, and external e-mail will be made available to all members and those officers with the authorisation of their director or head of service.

All use of e-mail shall be in accordance with the Electronic Communications Policy and Guidelines. Users shall avoid responding to unsolicited e-mails from unverifiable sources, and in particular, except where there is a justifiable business reason that has been expressly agreed with the ICT Manager, shall not open such mail or any attachments in such circumstances as there is a significant risk they may contain a virus. IT staff shall monitor usage of e-mail and report any concerns to the appropriate director or head of service.

All e-mail sent to external parties shall contain a standard disclaimer inserted by the e-mail system and in a form approved by the Council's Legal Officer.

All e-mail inbound and outbound will be subject to security scans for spyware, malware and viruses.

Electronic e-mail is not to be used via the Outlook App installed on personal devices.

Forwarding of e-mails to personal e-mail accounts is prohibited.

The use of personal e-mails for sharing of data is prohibited.

6.10.1 Confidential or RESTRICTED Information

Specific conditions apply to the use of RESTRICTED information:

- mail must not be forwarded to lower classification domains i.e. to organisations not within the government secure intranet network (GCSi) or government secure extranet (GCSx)

6.10.2 Use of E-mail Outside the UK

- **Due to the inherent increased security risk of accessing data via non-UK networks mail must not be accessed from outside the UK without the specific authorisation of the relevant Director.**
- Any user planning to do so must be aware of the relevant guidelines issued by FCO regarding the use of mobile telephones and IT services outside the UK.

6.11 Internet

Objective:

To facilitate use of this major source of information while preventing risks to the Council from inappropriate use:

The use of the Internet on the Council's computer systems shall be controlled and monitored to prevent:

- users wasting time and public resources by playing or "surfing" when they are paid to work;
- users accessing sites and importing material which the Council, as a matter of policy, may find unacceptable;
- users accessing sites and importing illegal material;
- users importing a virus or other malicious software and hence compromising the accuracy, availability and confidentiality of Council systems;
- users committing the Council to expenditure in an unauthorised fashion.

Internet access is to be used only for access to sites relevant to work or vocational training during an individual's working hours (this does not apply to members).

For staff in the main Council Offices this will be from 08:00 to 18:00 Monday to Friday. Officers using remote access facilities from home may use the Council's central internet connection between 07:00 and 22:30 on any day.

Personal use of the internet is permitted outside of staff's working hours and is subject to compliance with the Council's "Internet and E-mail Access - Conditions of Use" policy document.

This "Conditions of Use" policy will apply to those Members and Officers accessing the internet to view Web pages or to send / receive e-mails.

Internet access and e-mail is provided via a central connection to the internet which incorporates security features (intrusion detection and intrusion prevention) to safeguard the security and integrity of the Council's IT systems and data. This connection will always be used by Officers and members located at Council offices unless specifically authorised to use other methods. The key terms and conditions are as follows:

- Authority to use the Internet and/or e-mail facility will only be granted by the Chief Executive, Directors, Heads of Service or Service Managers.
- All Officers and Members using the facility will be required to sign the "Conditions of Use" document to confirm that they have read and agree to abide by its conditions. A breach of the conditions of use may result in disciplinary action and/or criminal proceedings.
- All "Conditions of Use" forms must be countersigned electronically or manually, by a designated authorising supervisor and completed documents will be held by the IT section and Human Resources section.
- All users of the facility will be issued with their own unique User ID and password and users will be deemed responsible for any activity logged against the user ID so User IDs and passwords should not be disclosed to other persons.
- The Council maintains logs of activity on our central Internet connection and may analyse and monitor those logs and all internet traffic.

Copies of the ‘conditions of use’ form are available on the Council’s intranet or are available from the ICT department.

All access to the Internet will be traceable to an originating user ID, both currently and retrospectively.

All access and attempted access to the Internet will be logged by the IT section, and comprehensive information on usage, including the time and length of visits, will be supplied on request or in the event of concerns by the ICT Manager, to a user’s director or head of service or Chief Executive in the case of members.

The IT section has implemented and maintains an automatic method for restricting which Internet sites may be accessed. No user shall attempt to access an Internet site which, from its address, may reasonably be considered to contain pornographic material or any other material prohibited by the **‘**Conditions of use” policy. The corporate leadership team will define which sites are not to be accessed and any deliberate attempt to access such site/s will be considered in accordance with the disciplinary procedure.

Intrusion protection system (IPS) is in place, to detect, monitor, analyse and alert on attempted cyber-attacks.

Access to restricted and prohibited sites is automatically monitored and reports of activity will be made available to the user’s director or head of service. A monthly security review will be conducted to ensure security and compliance, led by the ICT security officer.

The IT section has implemented and maintains a resilient security gateway device or "firewall" (software and hardware facilities) to control and vet and filter, incoming data to guard against recognised forms of Internet assaults and malicious software.

Only IT staff may download software, including freeware from the Internet. This does not apply to documents, i.e. Word, Excel, PDF format.

7. SYSTEM ACCESS CONTROL

7.1 Business Requirements for System Access

Objective:

To control access to business information:

Access to computer services and data should be controlled on the basis of business requirements, but accesses granted to a system should not compromise situations where separation (segregation) of duties is important.

Each system administrator will set up the system access rights of each user or group of users according to authorised business needs. Update access rights should be restricted to the minimum number of people commensurate with the need to maintain service levels.

System access controls are reviewed by Internal Audit during their routine systems audit work programme.

Domain privileged access will be reviewed periodically.

7.2 User Access Management

Objective:

To prevent unauthorised computer access:

Formal procedures will be developed for each system by the system administrator to cover the following:

- formal user registration and de-registration procedure for access to all multi-user IT services;
- restricted and controlled use of special privileges;
- Allocation of passwords securely controlled;
- ensuring the regular change and where appropriate quality and complexity of passwords;
- regular review of user access rights and privileged access rights;
- controlled availability of master passwords in emergencies.

A separate procedure document is available "Starters and Leavers Process Including Domain Account Administration" on the ICT intranet page.

User access will be suitably administered to ensure that the type of account granted to employees is such that it allows them to perform their day-to-day user activities and prevents access to any sensitive information not required for the purpose of undertaking their duties.

Ensuring members of staff, contractors and third party access to information systems does not exceed the needs of the role on a 'need to know' basis; that their use of ICT is appropriate and the starter, leaver and amendments changes are properly processed and authorised.

Network accounts which have not been logged into for 90 days will be reviewed and actioned taken. This activity will occur every 90 days to ensure accounts are disabled in quick and secure manner.

7.3 User Responsibilities

Objective:

To prevent unauthorised computer access:

Effective security requires the co-operation of authorised users. Users must comply with Council policies, standards and procedures regarding access controls, in particular the use of passwords and the security of equipment.

In order to maintain security users must:

- **not** write passwords down where others may readily discover them;
- **not** tell anyone else their password/s;
- **not** use obvious passwords such as their name;
- **not** let other people observe when entering their password;
- use a password with at least eight characters in it including numeric or special characters;
- promptly change their password if they suspect anyone else may be aware of it;
- log out of applications if they will be away from their desk for any length of time;
- 'lock' their PC when away from their desk to prevent it being used by others (by using Ctrl + Alt + Del keys or the Windows key + L key);
- if working at home the device must be shut down at the end of the day, so that security polices can be applied on next start up and stored in a secure location, when not in use;
- follow the Council's ICT security policy (including reading and signing confidentiality and conditions of use agreements);
- restart PCs and laptops as required after the application of security updates;
- report security incidents to the ICT Service Desk;
- not to open e-mails containing suspicions attachments;
- check e-mail and names of people they received a message from to ensure they are legitimate;
- report scams, privacy breaches and hacking attempts;
- do not re-use password from other systems.

Staff will be held responsible for all activities logged to their unique user ID.

7.4 Network Access Control

Objective:

Protection of networked services:

Connections to networked services shall be controlled in order to ensure that connected users or services do not compromise the security of any other networked services.

The ICT Manager is responsible for the protection of networked services.

All machines including servers are patched every month, this is the patch management cycle, to keep our estate up to date and protected.

A daily operations check is carried out as part of the daily checks procedure to ensure Antivirus, Antimalware and Anti Spyware updates are up to date on all PCs laptops and desktops

Devices not purchased by the ICT department are not to be plugged into or connected wirelessly to the Council's corporate network unless authorised by the ICT Manager or ICT Security officer.

All mobile devices and including tablets, laptops and smartphones will be encrypted using device management software.

7.5 Computer and Application Access Control

Objective:

To prevent unauthorised access to computers and information held:

Access to computer facilities should be restricted to authorised users. Computer facilities that serve multiple users should be capable of:

- identifying and verifying the identity of each authorised user, particularly where the user has update access;
- recording successful and unsuccessful attempts to access the system including files and folders;
- providing a password management system which ensures quality passwords;
- where appropriate restricting the connection times of users;
- controlling user access to data and system functions;
- restricting or preventing access to system utilities which override system or application controls;
- complete 'lock out' of user access after a pre-agreed number of unsuccessful attempts to access data.

8. SYSTEMS DEVELOPMENT AND MAINTENANCE

8.1 Security Requirements in Systems

Objective:

To ensure that security is built into IT systems and applications:

All security requirements, including a risk analysis and the need for fall back arrangements, should be identified at the requirements phase of a project by the officer requesting the system in consultation with computer and audit staff. Security requirements should be justified, agreed and documented.

The analysis of security requirements should:

- consider the need to safeguard the confidentiality, integrity and availability of information assets;
- identify controls to prevent, detect and recover from major failures or incidents;
- when specifying that a system requires a particular security feature, the quality of that feature must be specified, e.g. Password controlled - *"the password must be held in encrypted format. Passwords must expire after a number of days set by the system administrator, passwords should not be reusable, the system administrator should be able to specify a minimum length and other rules concerning password composition"*.

In order to ensure IT staff and users are aware of security controls in place, controls must be explicitly defined by the relevant system administrator in all relevant documentation.

8.2 Security of Application System Files

Objective:

To ensure that IT projects and support activities are conducted in a secure manner:

Access to application software, data files and system management files should be formalised and documented according to the sensitivity and importance of the system.

Maintaining the integrity of applications is the responsibility of the system administrator who will ensure that:

- strict control is exercised over the implementation of software on the operational system;
- test data is protected and controlled.

8.3 Security in Development and Support Environments

Objective:

To maintain the security of application systems software and data:

All proposed system changes must be reviewed to ensure they do not compromise the security of either the system or operating environment. The ICT Manager is responsible for all operating systems and the appropriate system administrator is responsible for the application. It is essential that both parties work together to ensure the security of application software and data is maintained.

Unsupported modifications to packaged software will only be authorised in exceptional circumstances. Wherever possible the required changes should be obtained from the vendor as standard program updates.

The implementation of any changes to systems should be strictly controlled using formal change control procedures. All system changes will be documented.

It should be a standard that any operational system has separate and secure test, training and development environments.

9. COMPLIANCE

9.1 Compliance with Legal Requirements and Codes of Practice

Objective:

The Council's statutory obligation to have sound information and cyber security arrangements in place originates in the Data Protection Act 1998, which states:

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and accidental damage or destruction of personal data."

The Council depends on the confidentiality, integrity and availability of its information and ICT to such an extent however, that a serious breach of information security could impact on the Council's ability to deliver a wide range of statutory services.

In addition the Council has contractual obligations to ensure sound security if it is to use the Government Public Services Network (PSN) or receive or share information with partner agencies under information sharing arrangement

There are a number of laws which relate directly or indirectly to IT and its use and it is essential that these statutory requirements are met. Legislation which applies includes:

- The Copyright, Designs and Patents Act 1988
- The Data Protection Act 1998
- The Computer Misuse Act 1996
- Regulation of Investigatory Powers Act 2000
- The Human Rights Act 1998
- Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000
- Health and Safety at Work etc Act 1974
- EC Directives.

In order to ensure security and integrity of data held and shared within both central government departments and local government the Council is obliged to adhere to set of standards defined in the 'code of connection' document issued by Department of Work and Pensions April 2008. The standard must be met before government departments such as Department of Work and Pensions will share data with the Council

Note: Failure to adhere to the required standard will result in electronic data sharing with government departments being suspended.

9.1.1 Control of Proprietary Software Copying

Objective:

To ensure that the Council complies with current legislation:

Proprietary software is usually supplied under a licence agreement which limits the number of users and/or limits the use to a specified machine. Copyright infringement can lead to legal action, fines and adverse publicity.

It is Council policy that no copyright material is copied without the owner's consent.

9.1.2 Use of Unlicensed Software

Except for freeware, the use of unlicensed software amounts to theft and the Council's policy is only to use licensed software. The Federation Against Software Theft (FAST) and the Business Software Alliance are particularly active in detecting and prosecuting organisations (especially councils) who use unlicensed software.

The introduction and/or use of unlicensed software is prohibited and may be treated as gross misconduct.

9.1.3 Safeguarding of the Council's Records

Important records must be protected from loss, destruction and falsification. All financial records need to be retained for seven years or more to meet audit requirements.

All historic data should be periodically archived by the relevant system administrator with copies being retained in media fire safes on and off site, in accordance with GDPR regulations.

9.1.4 Auditing and logging the use of ICT resources

The Council maintains audit logs of events taking place across its complete network. This includes, but not limited to:

- user login times;
- details if failed login attempts;
- details of access to data files and software applications (user ID, times);
- details of any privileged access to system;
- software and hardware configuration changes;
- details of internet web usage and restricted access reports;
- details of files, folder and network access to objects.

9.1.5 Data Protection

Personal information on living individuals who can be identified from the information that is stored or processed on a computer is subject to data protection legislation. The Data Protection Act 2018 extended this to information held in certain paper based systems. Disclosure of information is also governed by the Freedom of Information Act 2000.

The officer responsible within the Council for data protection is the Records Management Officer who will provide guidance to managers and other staff on their individual responsibilities and the specific procedures that should be followed.

It is a manager's responsibility to inform either the ICT Manager or the Records Management Officer of any proposals to keep personal information on a computer and any changes in the use for which data is kept. With the assistance of the Records Management Officer, managers must ensure that the relevant staff are made aware of the data protection principles defined in the legislation.

The Council is required to register details of the data kept, the purposes to which it is applied and to whom it may be disclosed. It is a manager's responsibility to ensure that the registration is accurate and amended when necessary and to take note of any advice from the Information Commissioner before undertaking any data matching exercise.

Under the Act staff could be held legally responsible for the confidentiality of personal data. Staff must be very careful as to whom they disclose information to and be aware of the need for security of information in any format including printed documents and electronic mail. **Particular care must be taken in disclosing personal data on the telephone, if in any doubt as to the identity of a caller personal data must not be disclosed on the telephone**.

The six principles of the Data Protection Act are that personal data should be:

- processed lawfully, fairly, and in a transparent manner relating to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

9.1.6 Prevention of Misuse of IT Facilities

The Council's computer facilities are provided for Council business or in connection with approved study courses. Staff and members are allowed to use the Council's computer facilities for personal use for the following:

- personal use of e-mail in accordance with the "Internet and E-Mail Access – Conditions of Use" policy document;
- access to the Internet, if granted for work purposes, in accordance with the Internet and E-Mail Access - Conditions of Use" policy document;
- limited use of PC software, particularly word processing, in their own time.

The following conditions will apply:

- all private printing must be paid for unless an agreement has been reached with the ICT Manager or the printing service;
- unauthorised or excessive personal use may be subject to disciplinary action;
- The Computer Misuse Act 1990 introduced three criminal offences:
  1. unauthorised access;
  2. unauthorised access with intent to commit a further serious offence;
  3. unauthorised modification of computer material, i.e. alteration, erasure or addition to programs or data.

Users should not attempt to gain access to systems they are not authorised to use or see, as they could face criminal prosecution.

9.2 Security Reviews of IT Systems

Objective:

To ensure compliance of systems with the Council's ICT and Cyber Security Policy and standards:

The internal and external security of IT systems including external penetration testing, will be regularly reviewed and subject to cyber security and penetration testing

This will be carried out by an approved CREST/IASME

The review of security processes will be carried out by Internal Audit, External Audit and managers

ICT will use specialist third parties to perform external and internal security and cyber security health checks, annually in order to maintain the Cyber Essential PLUS accreditation as well as meeting out PSN security obligations.

Annual reviews will ensure compliance and assurance with the security policy, standards and best practice.

9.3 System Audit Considerations

Objective:

To minimise interference to / from the system audit process:

Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimise the risk of disruptions to business processes.

There should be controls to safeguard operational systems and audit tools during system audits.

The following are to be observed:

- audit requirements to be agreed with the appropriate manager;
- the scope of any checks to be agreed and controlled;
- checks to be limited to read only access to software and data wherever possible;
- access, other than read only, only to be allowed for isolated copies of system files which must be erased when the audit is completed;
- IT resources for performing checks should be identified and made available;
- requirements for special or additional processing should be identified and agreed with service providers;
- wherever possible access should be logged and monitored;
- all procedures and requirements should be documented.

Access to system audit tools should be controlled.

APPENDIX 1

THE NATIONAL PROTECTIVE MARKING SCHEME FRAMEWORK

The National Protective Marking System provides a framework for users to share and protect information in an appropriate manner. As can be seen from the table, each protective marking is allocated an appropriate Impact Level (IL). Each IL describes a severity of impact to the UK of protectively marked information being released outside of normal government handling channels.

The IL value is used by security officers when performing a risk assessment on protectively marked information in order to determine how much protection these assets should be given.

Protective Marking	Impact Level
TOP SECRET	6
SECRET	5
CONFIDENTIAL	4
RESTRICTED	3
PROTECT	2 1
Unclassified	0

On 28 February 2007 the new sub-national caveat, PROTECT, was introduced. The purpose of PROTECT is to provide a difference in terms of the handling official information which needs to be protected from compromise of confidentiality, integrity and availability to a known level of assurance, but for which the measures required to safeguard National Security information at RESTRICTED are considered not to always meet the direct business need of the organisation. It is envisaged that in some organisations the use of RESTRICTED will be reduced as a consequence.

At the Local Authority level and for users of GCSx it is envisaged that most protectively marked information will be of 'PROTECT' in nature.

At a working level the baseline security objectives for PROTECT will be the same as for RESTRICTED, which are:

- handle, use and transmit with care;
- take basic precautions against accidental compromise or opportunist attack.

The distinction between the two markings is that PROTECT is not a National Security marking, and there is a revised calculation for asset value, or consequence of compromise. Depending on the severity of the circumstances either RESTRICTED or PROTECT may apply where compromise would be likely to:

- cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies;

- prejudice the investigation or facilitate the commission of crime;
- disadvantage government in commercial or policy negotiations with others.

N.B. Within the UK Government, CONFIDENTIAL is an explicit marking with clearly defined handling requirements. Sometimes, within certain local authorities 'Confidential' is used as a marking to indicate that information has a requirement for protection (in UK Government terms it is protectively marked). Care should be taken to ensure that information protectively marked with the national CONFIDENTIAL marking should be handled accordingly.

The PROTECT Classification

Guidelines	• Cause substantial distress to individuals. • Breach proper undertakings to maintain the confidence of information provided by third parties. • Breach statutory restrictions on the disclosure of information.
Principles and Clearance Levels	• Information classified as PROTECT should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely. • Only staff cleared by the organisation to access PROTECT level or above are authorised to handle the information. This includes all staff involved with transmission, storage and disposal.
Electronic Transmission	PROTECT information transmitted across public networks within the UK or across any networks overseas should be encrypted using an approved system.
Electronic Storage	Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms: a. User challenge and authentication (username / password or digital ID / Certificate). b. Logging use at level of individual. c. Firewalls and intrusion-detection systems and procedures; server authentication. d. OS-specific / application-specific security measures.
Electronic Disposal	Electronic files should be disposed of in a way that makes reconstruction highly unlikely.
Voice Telephone Conversation	Information protectively marked with PROTECT can be spoken about over the telephone.
Manual Transmission	• Within a single physical location. As determined by the information security officer. • Transfer between establishments within or outside UK**:** a. May be carried by ordinary postal service or commercial courier firms, provided the envelope / package is closed and the word PROTECT is not visible. b. The outer envelope should be addressed to an individual by name and title. PROTECT mail for / from overseas posts should be carried by diplomatic airfreight.

	c. The outer envelope must clearly show a return address in case delivery is unsuccessful. In some cases due to the nature of the contents, identifying the originating organisation may be inappropriate and a return PO Box alone should be used.
Manual Storage	• In an office environment, PROTECT material should be held in a lockable storage area or cabinet. • In a storage facility, all material should be protected through controlled access to the storage areas, and through a secure physical environment.
Manual Disposal	Disposed of or destroyed in a way that makes reconstruction highly unlikely.

The RESTRICTED Classification

Guidelines	• Affect diplomatic relations adversely. • Hinder the operational effectiveness or security of the UK or friendly forces. • Affect the internal stability or economic well-being of the UK or friendly countries adversely.
Principles and Clearance Levels	• Information classified as RESTRICTED should be held, processed, transmitted and destroyed with discretion to make compromise highly unlikely. • Only staff cleared by the organisation to access RESTRICTED level or above is authorised to handle the information. This includes all staff involved with transmission, storage and disposal.
Electronic Transmission	All RESTRICTED information transmitted across public networks within the UK or across any networks overseas must be encrypted using an approved system.
Electronic Storage	Electronic files (including databases) must be protected against illicit internal use or intrusion by external parties through a judicious selection of two or more of the following mechanisms: a. User challenge and authentication (username / password or digital ID / Certificate). b. Logging use at level of individual. c. Firewalls and intrusion-detection systems and procedures, server authentication. d. OS-specific / application-specific security measures.
Electronic Disposal	Electronic files should be disposed of in a way that makes reconstruction highly unlikely.
Voice Telephone Conversation	Telecommunications made at RESTRICTED (Confidentially IL 3) level can no longer be guaranteed as secure. Appropriate secure communications should be used.
Manual Transmission	• Within a single physical location. As determined by the information security officer.

	• Transfer between establishments within or outside UK**:** a. May be carried by ordinary postal service or commercial courier firms, provided the envelope / package is closed and the word RESTRICTED is not visible. b. The outer envelope should be addressed to an individual by name and title c. The outer envelope must show clearly a return address in case delivery is unsuccessful. In some cases, due to the nature of the contents, identifying the originating organisation may be inappropriate and a PO box should be used.
Manual Storage	• In an office environment, RESTRICTED material should be held in a lockable storage area or cabinet. • In a storage facility, all material should be protected through controlled access to the storage areas, and through a secure physical environment.
Manual Disposal	Disposed of or destroyed in a way that makes reconstruction highly unlikely.

Major Differences Between PROTECT and RESTRICTED

For Local authorities such as NWLDC the two protective markings which will be most commonly seen in the workplace are PROTECT and RESTRICTED. Out of these two protective markings it is anticipated that PROTECT will be the most common.

Information with the PROTECT protective marking will be handled in the same way as RESTRICTED in most circumstances. The primary difference is that Council Staff will be allowed to have telephone conversations with regard to information protectively marked as PROTECT. Information protectively marked as RESTRICTED is not allowed to be passed over the telephone.

SIGN BELOW TO ACCEPT THE ICT SECURITY POLICY AND HAND THE FORM TO THE ICT DEPARTMENT

North West Leicestershire District Council
Information and Communications Technology (ICT) and Cyber Security Policy

North West Leicestershire District Council is dependent upon its Information and Communications Technology (ICT) systems for its normal day to day business activities. It is therefore essential for the continued successful operation of the Council that the confidentiality, integrity and availability of its ICT systems and data are maintained at a high level. There is also an obligation on the Council and all employees, contractors and advisors to comply with the relevant legislation such as the Data Protection Acts, the Copyright, Designs and Patents Act and the Misuse of Computers Act.

It follows that a high standard of information security is required within the Council. To achieve this, the ICT and Cyber Security Policy has been adopted and everyone who uses IT equipment or accesses Council information must read the policy and ensure that they understand the obligations contained within it.

Once you have **read** and **understood** the ICT and Cyber Security Policy please sign and return the slip below to the ICT Service Desk.

North West Leicestershire District Council ICT and Cyber Security and Policy can be found on our intranet site

✂----------✂

North West Leicestershire District Council
Information and Communications Technology (ICT) and Cyber Security Policy

I have read and understand the North West Leicestershire District Council's ICT Security Policy.

Print Name _____ Signed _____ Date _____

(Note: When completed, this should be forwarded to the IT Section, who will copy it to the Human Resources Section)

APPENDIX 2

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL - GCSx PERSONAL COMMITMENT STATEMENT

I understand and agree to comply with the security rules of my organisation as well as the GCSx Code of Connection.

For the avoidance of doubt, the security rules relating to secure e-mail and IT systems usage include:

1. I acknowledge that my use of the GCSx may be monitored and/or recorded for lawful purposes.

2. I agree to be responsible for any use by me of the GCSx using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address.

3. I will not use a colleague's credentials to access the GCSx and will equally ensure that my credentials are not shared and are protected against misuse.

4. I will protect such credentials at least to the same level of secrecy as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises).

5. I will not attempt to access any computer system that I have not been given explicit permission to access.

6. I will not attempt to access the GCSx other than from IT systems and locations which I have been explicitly authorised to use for this purpose.

7. I will not transmit information via the GCSx that I know, suspect or have been advised is of a higher level of sensitivity than my GCSx domain is designed to carry.

8. I will not transmit information via the GCSx that I know or suspect to be unacceptable within the context and purpose for which it is being communicated.

9. I will not make false claims or denials relating to my use of the GCSx (e.g. falsely denying that an e-mail had been sent or received).

10. I will protect any sensitive or not protectively marked material sent, received, stored or processed by me via the GCSx to the same level as I would paper copies of similar material.

11. I will not send Protectively Marked information over public networks such as the Internet.

12. I will always check that the recipients of e-mail messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain.

13. I will not auto-forward e-mail from my GCSx account to any other non-GCSx e-mail account.

14. I will disclose information received via the GCSx only on a ‘need to know’ basis.

15. I will not forward or disclose any sensitive or protectively marked material received via the GCSx unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel.

16. I will seek to prevent inadvertent disclosure of sensitive or protectively marked information by avoiding being overlooked when working, by taking care when printing information received via the GCSx (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc) and by carefully checking the distribution list for any material to be transmitted.

17. I will securely store or destroy any printed material.

18. I will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via the GCSx (this might be by closing the e-mail program, logging-off from the computer, activate a password-protected screensaver, etc, so as to require a user logon for activation).

19. Where my organisation has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation), then I will not attempt to disable such protection.

20. I will make myself familiar with the security policies, procedures and any special instructions that relate to the GCSx.

21. I will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security.

22. I will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended.

23. I will not remove equipment or information from my employer’s premises without appropriate approval.

24. I will take precautions to protect all computer media and portable computers when carrying them outside my organisation’s premises (e.g. leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief).

25. I will not introduce viruses, Trojan horses or other malware into the system or GCSx.

26. I will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that my employer informs me are relevant.

27. If I am about to leave my employer, I will inform my manager prior to departure of any important information held in my account.

28. The GCSx Acceptable Usage Policy specifically states that all PROTECT and RESTRICT information will be appropriately labelled when sent over the GCSx and that public networks will not be used to send RESTRICT or PROTECT information.

29. I understand that use of GCSx / PSN services is subjected to Criminal conviction checks and I will declare any unspent convictions including cautions, reprimands, warnings, investigations or pending prosecutions to Human Resources.

PLEASE SGN BELOW TO ACCEPT THE GCSx SECURITY POLICY AND HAND THE FORM TO THE ICT DEPARTMENT

Name: ..... Dept: .....

Signed: .....Date: .....

Authorised: ..... Date: .....

This form can only be authorised by Team Managers or members of CLT.

(Note: When completed, this should be forwarded to the IT Section, who will copy it to the Human Resources Section)

APPENDIX 3

THIRD PART NETWORK ACCESS AGREEMENT

1. Purpose

The purpose of this agreement is to outline the specific terms and conditions governing the access and use of the North West Leicestershire District Council (NWLDC) network and information technology resources by the Third Party.

This agreement is dated and made between **North West Leicestershire District Council** and the following Third Party:

Company name:	[	]
Address:	[	]
	[	]
	[	]
Contact Name:	[	]
Phone number:	[	]
E-mail address:	[	]

2. Definitions

Third parties are defined as any individual, consultant, contractor, vendor or agent not registered as a NWLDC employee.

Third party access is defined as all local or remote access to the NWLDC network for any purpose.

NWLDC network includes all data, applications, systems, services, infrastructure and computer devices which are owned or leased by the NWLDC.

Mobile computer devices are defined as any handheld computer device, including but not limited to laptops, notebooks, tablet computers, smartphone devices (e.g. PDA, iPhone and Blackberry enabled devices, etc).

Removable storage devices are defined as any optical or magnetic storage device or media, including but not limited to floppy disks, CD, DVD, magnetic tapes, ZIP disk, USB flash drive (i.e. memory stick / pen / keys), external / portable hard drives and SD Cards.

3. Terms and Conditions

In consideration of NWLDC engaging the Third Party for services requiring third party access and allowing such third party access, the Third Party agrees to the following:

(a) The Third Party may only use the network connection for approved business purposes as specified by NWLDC and in accordance with NWLDC ICT policies. The use of the network connection for unapproved purposes, including but not limited to personal use or gain is strictly prohibited.

(b) The Third Party may only use access methods which have been defined by the NWLDC ICT Services.

(c) The Third Party must ensure that only their employees that have been nominated by the Third Party and approved by the NWLDC in advance, have access to the network connection or any NWLDC owned equipment.

(d) The Third Party shall be solely responsible for ensuring its nominated employees are not security risks, and upon request from the NWLDC, the Third Party will provide the NWLDC with any information reasonably necessary for the NWLDC to evaluate security issues.

(e) The Third Party will promptly inform the NWLDC in writing of any relevant employee changes. This includes the rotation and resignation of employees so that NWLDC can disable their usernames and remove / change passwords in order to secure its resources.

(f) As part of any service agreement review the Third Party will provide the NWLDC with an up to date list of their employees who have access to the network connection or any NWLDC owned equipment.

(g) The Third Party is solely responsible for ensuring that all usernames and passwords issued to them by the NWLDC remain confidential and are not used by unauthorised individuals. The Third Party must immediately contact NWLDC if they suspect these details have been compromised.

(h) The Third Party will be held responsible for all activities performed on the NWLDC network while logged in under their usernames and passwords.

(i) The Third Party must ensure at all times that all computer devices used by them to connect to the NWLDC network have reputable up to date anti-virus software and the appropriate security patches installed.

(j) Only in exceptional circumstances and with the prior written approval of the NWLDC should the Third Party hold NWLDC information on mobile computer devices or removable storage devices. Should the business requirements necessitate the Third Party to store NWLDC information on mobile computer devices or removable storage devices, the Third Party must ensure that only the absolute minimum amount of information as is absolutely necessary is stored on the mobile computer device or removable storage device and the information is securely deleted when it is no longer required. The Third Party must ensure that all NWLDC information stored on mobile computer devices and removable storage devices belonging to the Third Party is encrypted to standards approved by NWLDC. Under no circumstance encrypted or otherwise should NWLDC information be stored by the Third Party on USB memory keys / sticks.

(k) The Third Party must ensure that all mobile computer devices used by them to connect to the NWLDC network, are used in such a way that information belonging to the NWLDC is not displayed to unauthorised individuals or the general public.

(l) The Third Party must ensure that all their computer devices connected to the NWLDC network are not connected to any other network at the same time, with the exception of networks that are under the complete control of the Third Party.

(m) When the Third Party is connected to the NWLDC network they should not leave their computer devices unattended.

(n) The Third Party must ensure that when they are connected to NWLDC network their activity does not disrupt or interfere with other non-related network activity.

(o) All Third Party computer devices used to connect to the NWLDC network must, upon request by NWLDC be made available for inspection.

(p) The Third Party network connection will by default be granted read / execute privileges only. All requests for increased privileges must be submitted in writing to the NWLDC where they will be considered on a case by case basis.

(q) For security reasons all Third Party remote access accounts except those providing 24*7 support may be switched off (de-activated) by default. The Third Party will be required to e-mail (can be followed by phone) NWLDC ICT Services requesting that their account be switched-on (activated) for a stipulated period.

(r) The Third Party must obtain the written consent of the NWLDC before implementing any updates or amendments to the NWLDC network, information systems, applications or equipment. All approved updates and amendments implemented by the Third Party must be made in line with NWLDC policies and procedures.

(s) The Third Party must ensure all software is scanned and cleared of all viruses and other forms of malicious software before it is installed on any NWLDC information systems, applications or equipment. The Third Party will be held responsible for all disruptions and damage caused to the NWLDC network, information systems, applications or equipment which is traced back to infected software installed by the Third Party.

(t) The Third Party and their employees must comply with all UK, European and NWLDC rules and regulations concerning safety, environmental and security operations while on-site at an NWLDC site. All Third Party personnel must carry photographic identification with them when they are on-site at an NWLDC facility.

(u) Where the Third Party has direct or indirect access to NWLDC information, this information must not be copied, divulged or distributed to any other party without the prior written approval of the NWLDC.

(v) The Third Party must report all actual and suspected security incidents to the NWLDC immediately.

(w) The Third Party must manage and process all NWLDC information which they acquire from the NWLDC in accordance the Data Protection Act 1998 (as amended or replace) and any associated guidance.

(x) The NWLDC reserves the right to:

- Monitor all Third Party activity while connected (local and remote) to the NWLDC network.
- Audit contractual responsibilities or have those audits carried out by an NWLDC approved third party
- Revoke the Third Party's access privileges at any time.

(y) On completion of the services requiring third party access, the Third Party must return all equipment, software, documentation and information belonging to the NWLDC.

(z) Any violations of this agreement by the Third Party, may lead to the withdrawal of NWLDC network and information technology resources to that Third Party and/or the cancellation of any contract(s) between the NWLDC and the Third Party.

The Third Party agrees to abide by the terms and conditions of this agreement at all times.

Signed (On behalf of the Third Party):

Authorised Signature: .....

Name (Printed): .....

Title or Position: .....

Date: .....

This page is intentionally left blank

NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL
Local Code of Corporate Governance

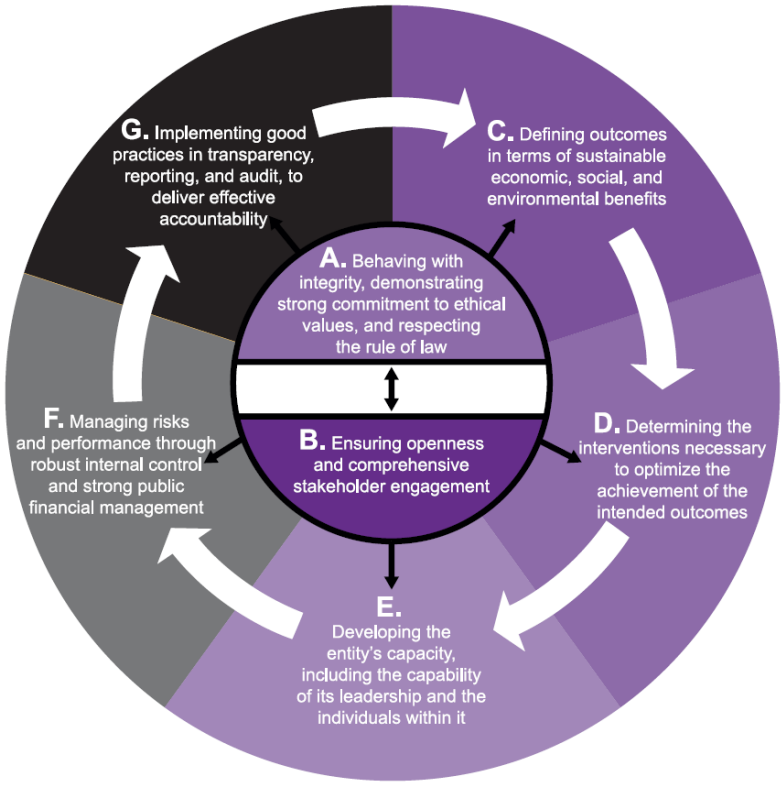
1 INTRODUCTION

1.1 In 2014, the Chartered Institute of Public Finance and Accountancy (CIPFA) and the International Federation of Accountants (IFAC) collaborated to produce The International Framework: Good Governance in the Public Sector. The International Framework defines governance as comprising the arrangements put in place to ensure that intended outcomes for stakeholders are defined and achieved. It states that in order to deliver good governance in the public sector, both governing bodies and individuals working for public sector entities must try to achieve their entity's objectives while acting in the public interest at all times.

1.2 The Chartered Institute of Public Finance and Accountancy in association with SOLACE have published their Framework entitled 'Delivering Good Governance in Local Government 2016'.

1.3 The diagram below[1] illustrates the core principles of good governance in the public sector and how they relate to each other: Principles A and B permeates implementation of principles C to G.

Achieving the Intended Outcomes While Acting in the Public Interest at all Times



[1] CIPFA/SOLACE Delivering Good Governance in Local Government Framework 2016

1.4 In North West Leicestershire, good governance is about how the Council ensures that it is doing the right things, in the right way and for the benefit of the communities it serves. The starting place for good governance is having shared values and culture and a framework of overarching strategic policies and objectives underpinned by robust systems and processes for delivering these.

1.5 By ensuring good governance is in place, the Council will ensure it has high standards of management, strong performance, the effective use of resources and good outcomes which in turn will lead to increased public trust.

1.6 The Council is committed to the seven core principles of good practice contained in the CIPFA framework and will test its governance arrangements against this framework and report annually (via its annual assurance review and Annual Governance Statement).

2 SUMMARY OF COMMITMENT

2.1 By adopting this Local Code of Corporate Governance, we are responding to the CIPFA/SOLACE Joint Working Group Guidance and Framework entitled 'Delivering Good Governance in Local Government'.

2.2 In doing so we will:

- Accept the core principles set out in section 3 below as the basis for our Corporate Governance arrangements.
- Publish an Annual Governance Assurance Statement with the Council's Statement of Accounts.
- Draw up Action Plans of improvements to our corporate governance arrangements, such plans to be monitored by the Audit and Governance Committee.

3 FUNDAMENTAL PRINCIPLES OF CORPORATE GOVERNANCE

3.1 Set out in this document is the Council's proposed Local Code of Corporate Governance which is based on the seven core principles (as set out in the illustration above) adopted for local government from the report of the Independent Commission on Good Governance in Public Services.

Principle A - Behaving with integrity, demonstrating strong commitment to ethical values, and respecting the rule of law

The Council is committed to:

Behaving with Integrity

- Ensuring members and officers behave with integrity and lead as a culture where acting in the public interest is visibly and consistently demonstrated thereby protecting the reputation of the organisation.
- Ensuring members take the lead in establishing specific standard operating principles or values for the organisation and its staff and that they are communicated and understood. These should build on the Seven Principles of Public Life (The Nolan Principles).
- Leading be example and using these standard operating principles or values as a framework for decision making and other actions.
- Demonstrating, communicating and embedding the standard operating principles or values through appropriate policies and processes which are reviewed on a regular basis to ensure they are operating effectively.

Demonstrating strong commitment and ethical values

- Seeking to establish, monitor and maintain the organisation's ethical standards and performance
- Underpinning personal behaviour with ethical values and ensuring they permeate all aspects of the organisation's culture and operation
- Developing and maintaining robust policies and procedures which place emphasis on agreed ethical values
- Ensuring that external providers of services on behalf of the organisation are required to act with integrity and in compliance with high ethical standards expected by the organisation

Respecting the rule of law

- Ensuring members and staff demonstrate a strong commitment to the rule of the law as well as adhering to relevant laws and regulations
- Creating the conditions to ensure that the statutory officers, other key post holders and members are able to fulfil their responsibilities in accordance with legislative and regulatory requirements
- Striving to optimise the use of the full powers available for the benefit of citizens, communities and other stakeholders
- Dealing with breaches of legal and regulatory provisions effectively
- Ensuring corruption and misuse of power are dealt with effectively

Principle B – Ensuring openness and comprehensive stakeholder engagement

The Council is committed to:

Openness

- Ensuring an open culture through demonstrating, documenting and communicating the organisation's commitment to openness
- Making decisions that are open about actions, plans, resource use, forecasts, outputs and outcomes. The presumption is for openness. If that is not the case, a justification for the reasoning for keeping a decision confidential should be provided
- Providing clear reasoning and evidence for decisions in both public records and explanations to stakeholders and being explicit about the criteria, rationale and considerations used. In due course, ensuring that the impact and consequences of those decisions are clear
- Using formal and informal consultation and engagement to determine the most appropriate and effective interventions/ courses of action

Engaging comprehensively with institutional stakeholders

- Effectively engaging with institutional stakeholders to ensure that the purpose, objectives and intended outcomes for each stakeholder relationship are clear so that outcomes are achieved successfully and sustainably
- Developing formal and informal partnerships to allow for resources to be used more efficiently and outcomes achieved more effectively
- Ensuring that partnerships are based on: trust, a shared commitment to change, a culture that promotes and accepts challenge among partners and that the added value of partnership working is explicit

Engaging stakeholders effectively, including individual citizens and service users

- Establishing a clear policy on the type of issues that the organisation will meaningfully consult with or involve individual citizens, service users and other stakeholders to ensure that service (or other) provision is contributing towards the achievement of intended outcomes.
- Ensuring that communication methods are effective and that members and officers are clear about their roles with regard to community engagement
- Encouraging, collecting and evaluating the views and experiences of communities, citizens, service users and organisations of different backgrounds including reference to future needs
- Implementing effective feedback mechanisms in order to demonstrate how their views have been taken into account
- Balancing feedback from more active stakeholder groups with other stakeholder groups to ensure inclusivity
- Taking account of the interests of future generations of tax payers and service users

Principle C – Defining outcomes in terms of sustainable economic, social, and environmental benefits

The Council is committed to:

Defining outcomes

- Having a clear vision which is an agreed formal statement of the organisation's purpose and intended outcomes containing appropriate performance indicators, which provides the basis for the organisation's overall strategy, planning and other decisions
- Specifying the intended impact on, or changes for, stakeholders including citizens and service users. It could be immediately or over the course of a year or longer
- Delivering defined outcomes on a sustainable basis within the resources that will be available
- Identifying and managing risks to the achievement of outcomes
- Managing service users expectations effectively with regard to determining priorities and making the best use of the resources available

Sustainable economic, social and environmental benefits

- Considering and balancing the combined economic, social and environmental impact of policies, plans and decisions when taking decisions about service provision
- Taking a longer-term view with regard to decision making, taking account of risk and acting transparently where there are potential conflicts between the organisation's intended outcomes and short-term factors such as the political cycle or financial constraints
- Determining the wider public interest associated with balancing conflicting interests between achieving the various economic, social and environmental benefits, through consultation where possible, in order to ensure appropriate trade-offs
- Ensuring fair access to services

Principle D – Determining the interventions necessary to optimise the achievement of the intended outcomes

The Council is committed to:

Determining interventions

- Ensuring decision makers receive objective and rigorous analysis of a variety of options indicating how intended outcomes would be achieved and including the risks associated with those options. Therefore ensuring best value is achieved however services are provided
- Considering feedback from citizens and service users when making decisions about service improvements or where services are no longer required in order to prioritise competing demands within limited resources available including people, skills, land and assets and bearing in mind future impacts

Planning interventions

- Establishing and implementing robust planning and control cycles that cover strategic and operational plans, priorities and targets
- Engaging with internal and external stakeholders in determining how services and other courses of action should be planned and delivered
- Considering and monitoring risks facing each partner when working collaboratively including shared risks
- Ensuring arrangements are flexible and agile so that the mechanisms for delivering outputs can be adapted to changing circumstances
- Establishing appropriate key performance indicators (KPIs) as part of the planning process in order to identify how the performance of services and projects is to be measured
- Ensuring capacity exists to generate the information required to review service quality regularly
- Preparing budgets in accordance with organisational objectives, strategies and the medium term financial plan Informing medium and long term resource planning by drawing up realistic estimates of revenue and capital expenditure aimed at developing a sustainable funding strategy

Optimising achievement of intended outcomes

- Ensuring the medium term financial strategy integrates and balances service priorities, affordability and other resource constraints
- Ensuring the budgeting process is all-inclusive, taking into account the full cost of operations over the medium and longer term
- Ensuring the medium term financial strategy sets the context for ongoing decisions on significant delivery issues or responses to changes in the external environment that may arise during the budgetary period in order for outcomes to be achieved while optimising resource usage
- Ensuring the achievement of ‘social value’ through service planning and commissioning.

Principle E – Developing the entity's capacity, including the capability of its leadership and the individuals within it

The Council is committed to:

Developing the entity's capacity

- Reviewing operations, performance use of assets on a regular basis to ensure their continuing effectiveness
- Improving resource use through appropriate application of techniques such as benchmarking and other options in order to determine how the authority's resources are allocated so that outcomes are achieved effectively and efficiently
- Recognising the benefits of partnerships and collaborative working where added value can be achieved
- Developing and maintaining an effective workforce plan to enhance the strategic allocation of resources

Developing the capability of the entity's leadership and other individuals

- Developing protocols to ensure that elected and appointed leaders negotiate with each other regarding their respective roles early on in the relationship and that a shared understanding of roles and objectives is maintained
- Publishing a statement that specifies the types of decisions that are delegated and those reserved for the collective decision making of the governing body
- Ensuring the leader and the chief executive have clearly defined and distinctive leadership roles within a structure whereby the chief executive leads the authority in implementing strategy and managing the delivery of services and other outputs set by members and each provides a check and a balance for each other's authority
- Developing the capabilities of members and senior management to achieve effective shared leadership and to enable the organisation to respond successfully to changing legal and policy demands as well as economic, political and environmental changes and risks by:
    - ensuring members and staff have access to appropriate induction tailored to their role and that ongoing training and development matching individual and organisational requirements is available and encouraged
    - ensuring members and officers have the appropriate skills, knowledge, resources and support to fulfil their roles and responsibilities and ensuring that they are able to update their knowledge on a continuing basis
    - ensuring personal, organisational and system-wide development through shared learning, including lessons learnt from governance weaknesses both internal and
- Ensuring that there are structures in place to encourage public participation
- Taking steps to consider the leadership's own effectiveness and ensuring leaders are open to constructive feedback from peer review and inspections
- Holding staff to account through regular performance reviews which take account of training or development needs Ensuring arrangements are in place to maintain the health and wellbeing of the workforce and support individuals in maintaining their own physical and mental wellbeing

Principle F – Managing risks and performance through robust internal control and strong public financial management

The Council is committed to:

Managing risk

- Recognising that risk management is an integral part of all activities and must be considered in all aspects of decision making
- Implementing robust and integrated risk management arrangements and ensuring that they are working effectively
- Ensuring that responsibilities for managing individual risks are clearly allocated

Managing performance

- Monitoring service delivery effectively including planning, specification, execution and independent post implementation review
- Making decisions based on relevant, clear objective analysis and advice pointing out the implications and risks inherent in the organisation's financial, social and environmental position and outlook
- Ensuring an effective scrutiny or oversight function is in place which encourages constructive challenge and debate on policies and objectives before, during and after decisions are made thereby enhancing the organisation's performance and that of any organisation for which it is responsible (OR, for a committee system) Encouraging effective and constructive challenge and debate on policies and objectives to support balanced and effective decision making
- Providing members and senior management with regular reports on service delivery plans and on progress towards outcome achievement
- Ensuring there is consistency between specification stages (such as budgets) and post implementation reporting (e.g. financial statements)

Robust internal control

- Aligning the risk management strategy and policies on internal control with achieving the objectives
- Evaluating and monitoring the authority's risk management and internal control on a regular basis
- Ensuring effective counter fraud and anti-corruption arrangements are in place
- Ensuring additional assurance on the overall adequacy and effectiveness of the framework of governance, risk management and control is provided by the internal auditor
- Ensuring an audit committee or equivalent group or function which is independent of the executive and accountable to the governing body: provides a further source of effective assurance regarding arrangements for managing risk and maintaining an effective control environment that its recommendations are listened to and acted upon

Managing Data

- Ensuring effective arrangements are in place for the safe collection, storage, use and sharing of data, including processes to safeguard personal data
- Ensuring effective arrangements are in place and operating effectively when sharing data with other bodies
- Reviewing and auditing regularly the quality and accuracy of data used in decision making and performance monitoring

Strong public financial management

- Ensuring financial management supports both long term achievement of outcomes and short-term financial and operational performance
- Ensuring well-developed financial management is integrated at all levels of planning and control, including management of financial risks and controls

Principle G – Implementing good practices in transparency, reporting, and audit to deliver effective accountability

The Council is committed to:

Implementing good practice in transparency

- Writing and communicating reports for the public and other stakeholders in an understandable style appropriate to the intended audience and ensuring that they are easy to access and interrogate
- Striking a balance between providing the right amount of information to satisfy transparency demands and enhance public scrutiny while not being too onerous to provide and for users to understand

Implementing good practice in reporting

- Reporting at least annually on performance, value for money and the stewardship of its resources
- Ensuring members and senior management own the results
- Ensuring robust arrangements for assessing the extent to which the principles contained in the Framework have been applied and publishing the results on this assessment including an action plan for improvement and evidence to demonstrate good governance (annual governance statement)
- Ensuring that the Framework is applied to jointly managed or shared service organisations as appropriate
- Ensuring the performance information that accompanies the financial statements is prepared on a consistent and timely basis and the statements allow for comparison with other similar organisations

Assurance and effective accountability

- Ensuring that recommendations for corrective action made by external audit are acted upon
- Ensuring an effective internal audit service with direct access to members is in place which provides assurance with regard to governance arrangements and recommendations are acted upon
- Welcoming peer challenge, reviews and inspections from regulatory bodies and implementing recommendations
- Gaining assurance on risks associated with delivering services through third parties and that this is evidenced in the annual governance statement
- Ensuring that when working in partnership, arrangements for accountability are clear and that the need for wider public accountability has been recognised and met

4 REVISIONS OF THE LOCAL CODE

4.1 The contents of this Local Code will be reviewed when necessary usually on an annual basis.

NWLDC
REVIEWED AND UPDATED – FEBRUARY 2008
REVIEWED – JUNE 2009
REVIEWED AND UPDATED – SEPTEMBER 2017

This page is intentionally left blank

MINUTES of a meeting of the AUDIT AND GOVERNANCE COMMITTEE held in the Remote meeting using Microsoft Teams on WEDNESDAY, 22 JULY 2020

Present: Councillor S Gillard (Chairman)

Councillors D Harrison, C C Benfield, D Bigby, J Clarke, M D Hay, K Merrie MBE, V Richichi and S Sheahan

Officers: Mrs T Bingham, Miss A Wright, Mrs L Marron, Miss E Warhurst, Mr T Delaney and Mrs R Wallace

External Audit: Mr M Surridge

1. APOLOGIES FOR ABSENCE

Apologies for absence were received from Councillor M B Wyatt.

2. DECLARATION OF INTERESTS

There were no declarations of interest.

3. MINUTES

Consideration was given to the minutes of the meeting held on 17 March 2020.

It was moved by Councillor S Sheahan, seconded by Councillor D Harrison and

RESOLVED THAT:

The minutes of the meeting held on 17 March 2020 be approved as a correct record and signed by the Chairman.

4. EXTERNAL AUDIT PROGRESS REPORT

The External Auditor presented the report detailing the progress to date, and highlighted the changes in accounts and audit timetable due to the pension element. He also referred Members to the financial reporting issues in relation to Covid-19.

In response to questions, the Head of Finance explained that a report in relation to the impact of Covid-19 on the financial forecast was due to be considered by Cabinet the following day, with a more up to date forecast going to the Cabinet meeting in September as part of quarterly reporting. Her opinion as Section 151 Officer was that the Council is well equipped to deal with the financial challenges.

The External Auditor gave an explanation on his role and the audit fee for the benefit of new members of the committee.

The Chairman thanked the External Auditor for his attendance.

5. INTERNAL AUDIT PROGRESS REPORT

The Audit Manager presented the report, highlighting the work undertaken in Quarter 1. Members noted that work had not yet begun on the 2020/21 plan due to Covid-19 and the Council's business focus on critical services, therefore there was no movement shown in Appendix A.

In relation to the Affordable Housing – S106/Commuted Sums recommendation at Appendix B, Councillor D Bigby asked if once completed, it would be published and available both to councillors and the public. The Audit Manager was unable to confirm but believed that once formal agreement had been reached, it would be publically available.

Councillor K Merrie raised concerns regarding the high priority rated Health and Safety Welfare recommendation, detailed at Appendix C, for which the completion date had been extended for a second time. He asked why it was yet to be completed and if the Council had the support required. The Audit Manager explained that it was still included on the tracker as it was only partly implemented. A new health and safety system has been introduced but unfortunately, due to Covid-19, it had not been fully rolled out and was not being used to its full potential. Therefore, it had been kept on the tracker to allow a follow up at a future date. Councillor K Merrie raised further strong concerns regarding the incompletion of this recommendation.

The Head of Finance reminded members that any Head of Service could be invited to committee at any time regarding a particular recommendation if desired. After a prompt from the Chairman, Members agreed for the Head of Human Resources and Organisational Development to be invited to the next meeting to discuss the Health and Safety recommendation further.

Councillor J Clarke asked if any S106 monies were due to expire shortly and if impacted by Covid-19, would the money be lost. The Head of Finance agreed to take the question back to officers and provide an answer outside of the meeting.

It was moved by Councillor D Harrison, seconded by Councillor J Clarke and

RESOLVED THAT:

The report be noted.

6. INTERNAL AUDIT ANNUAL REPORT

The Audit Manager presented the annual report, summarising the work of internal audit carried out during 2019/20, issues relevant to the preparation of the Annual Governance Statement, Internal Audit's Quality Assurance Improvement Programme and statement of conformance with the Public Sector Internal Audit Standards. She also highlighted her required annual opinion, as Audit Manager, on the overall adequacy and effectiveness of the organisations framework of governance, risk management and control.

The Audit Manager also informed Members of the next external audit inspection scheduled to take place in November 2020.

In response to a question from Councillor D Bigby, the Audit Manager explained that the last external inspection was carried out through CIPFA and this one would be conducted by Elizabeth Humphries, a very experienced assessor who carried out the previous inspection in 2015.

It was moved by Councillor J Clarke, seconded by Councillor D Bigby and

RESOLVED THAT:

The report be noted.

7. TREASURY MANAGEMENT STEWARDSHIP REPORT 2019/20

The Finance Team Manager presented the report, detailing the Council's treasury position, as well as the borrowing, debt rescheduling and investment activity.

In response to a question from Councillor D Bigby, the Finance Team Manager explained that the same protection applied to local authority investments as to the investments.

In response to a question from Councillor S Sheahan regarding the decision to invest more in Local Authorities rather than banks to lower the inherent investment risk, the Finance Team Manager explained that the decision was made at the advice of the Council's external advisor as a safer investment. The Head of Finance confirmed this and added that this was due to "bail-in" risk. Following a further comment from Councillor S Sheahan, the Head of Finance confirmed that assurances were sought on all advice given to ensure it was sound.

In reference to Appendix A, credit review and banks sovereign ratings, Councillor C Benfield questioned if the rating was to deteriorate, would it affect the Council's borrowing. The Finance Team Manager responded that as the current borrowing was at a fixed rate, a change would not have an impact but it could on any future investments.

In response to a further question from Councillor C Benfield regarding ethical measures used when investing, it was confirmed that there were currently no ethical measures in the framework but it was something that was being looked at due to its rise in interest.

It was moved by Councillor S Gillard, seconded by Councillor D Harrison and

RESOLVED THAT:

The report be approved.

8. PROGRESS OF IMPROVEMENTS IDENTIFIED THROUGH ANNUAL GOVERNANCE REVIEW 2018/19

The Head of Finance presented the report. She reminded Members that the report was deferred from the previous meeting as the agenda was shortened due to the emerging pandemic social distancing measures and therefore was a little out of date. At the time of writing the report, four improvements had been completed and five were underway. Members were informed that the Annual Governance Statement 2019/20 had now been completed and published, and three of the improvements underway had been carried forward to 2020/21.

It was moved by Councillor K Merrie, seconded by Councillor D Harrison and

RESOLVED THAT:

The report be noted.

9. REVIEW OF CORPORATE POLICIES

The Head of Finance presented the report, referring members to the corporate polices listed with the dates they were last reviewed at paragraph 1.2 of the report and the summary of changes to each policy at section 2.0 of the report.

In response to a question from Councillor D Bigby, the Head of Finance confirmed that the policies predominantly related to staff but the Data Protection Policy and ICT/Cyber Security Policy also related to Members. The Head of Legal and Commercial Services reminded Members that they had signed to adhere to these policies after they were

Chairman's initials

elected and information was provided in their induction packs. She added that once the policy changes had been agreed by Cabinet, Members would be sent the relevant updated policy documents with the changes highlighted for information. It was confirmed that Members would not be required to sign up to the policies again as they had already made the commitment.

Councillor J Clarke drew attention to the Council owned drone referred to at paragraph 2.5 of the report and asked how it was used. The Head of Legal and Commercial Services explained that the drone was predominantly used by the Planning Enforcement Team to view sites that were inaccessible.

In relation to the Anti-Money Laundering Policy, Councillor C Benfield asked if contractors are made to sign anything when selected. The Head of Finance explained that contractors are not asked to specifically sign anything but adherence to the Council's policies were covered as part of the procurement process.

All comments be presented to Cabinet when it considered the report at its meeting on 22 September 2020.

10. STANDARDS AND ETHICS - QUARTER 3 REPORT

The Head of Legal and Commercial Services presented the report and reminded Members that this was also deferred from the last meeting for the same reason as explained earlier.

It was moved by Councillor S Gillard, seconded by Councillor C Benfield and

RESOLVED THAT:

The report be noted.

11. STANDARDS AND ETHICS - QUARTER 4 REPORT

The Head of Legal and Commercial Services presented the report.

It was moved by Councillor S Gillard, seconded by Councillor D Harrison and

RESOLVED THAT:

The report be noted.

12. STANDARDS AND ETHICS - QUARTER 1 REPORT

The Head of Legal and Commercial Services presented the report and highlighted the changes to the format following comments from Members. She also referred to the RIPA information, which had been put back into the report following a recommendation from the ICO during an inspection earlier in the year.

In response to a question from Councillor M Hay regarding the information available on Freedom of Information exemptions used by the Council, the Head of Legal and Commercial Services agreed to include more detail in future reports in relation to the categories of exemptions used and the numbers in each category.

It was moved by Councillor S Gillard, seconded by Councillor V Richichi and

RESOLVED THAT:

The report be noted.

13. DRAFT MEMBER CONDUCT ANNUAL REPORT

The Head of Legal and Commercial Services presented the report and referred Members to the list of policies and procedures as detailed at section 7.0 of the report.

Members were informed that following the ballot for the Parish Representatives on the Committee, the count was held prior to the meeting in the presence of the Chairman and the Monitoring Officer. The successful candidates would be informed by letter later in the week and formally appointed at the next Council meeting.

It was moved by Councillor S Gillard, seconded by Councillor J Clarke and

RESOLVED THAT:

a) The report be noted.

b) Authority to make any minor amendments to the report following comments from the Committee be delegated to the Head of Legal and Commercial Services.

RECOMMENDED THAT:

c) Council endorse the Member Conduct Annual Report 2019/20.

14. REVIEW OF THE MODEL CODE OF CONDUCT

The Head of Legal and Commercial Services presented the report, summarising the LGA consultation and its aims. District and Parish Councillors had already been invited to comment and it had been brought to the meeting to give committee members the opportunity to provide feedback also. It was suggested that a small task and finish group be established to consider the council's response to the consultation, with membership to be sought outside of the meeting by Democratic Services.

In response to a question from Councillor C Benfield, the Head of Legal and Commercial Services confirmed that a high proportion of the Parish Councils implemented the District member Code of Conduct or with very minor differences.

A number of Members were unable to open the PDF document links included in the report and therefore it was agreed for Democratic Services to circulate the documents by email.

It was moved by Councillor S Sheahan, seconded by Councillor D Harrison and

RESOLVED THAT:

A task and finish group be established to consider the LGA's Review of the Model Code of Conduct.

15. UPDATE OF THE COUNCIL'S CONSTITUTION

The Head of Legal and Commercial Services presented the report, highlighting the proposed changes to the Constitution as detailed at section 2.0 of the report.

Members were also informed of the recent changes to the Business and Planning Bill in relation to the provisions to the promotion of economic growth, such as pavement licences. Amendments introduced during the reading of the Bill in the House of Lords meant that these functions would become executive functions and therefore work would be required to look at delegations needed to manage the licensing process. If the Bill received wide ascent later in the week a decision would need to be made regarding the use of some urgent powers of the Chief Executive to manage the process in the meantime before it was considered at Council in September.

Councillor D Bigby welcomed the clarification of the allowance of questions by members of the public at the Local Plan Committee. He also referred to the provision of papers to Councillors in the Remote Meeting Procedure Rules, as he currently could not access all confidential reports. It was agreed for Democratic Services to investigate Councillor D Bigby's system access to ensure all confidential papers were available to him.

In response to a comment from Councillor D Bigby regarding paragraph 3.1 of the Remote Meeting Procedure Rules, it was agreed to look at the wording to make it clear that it was Members in attendance that would be regarded as present for the purposes of determining a quorum, not those authorised.

It was moved by Councillor J Clarke, seconded by Councillor C Benfield and

RECOMMENDED THAT COUNCIL:

a) Adopt the amendments to the Constitution as set out in the report.

b) Authorises the Head of Legal and Commercial Services to make the agreed amendments and any consequential amendments to the Constitution and re-issue the document.

16. COMMITTEE WORK PLAN

The Committee considered its current work plan.

By affirmation of the meeting it was

RESOLVED THAT:

The committee work plan be noted.

The meeting commenced at 6.30 pm

The Chairman closed the meeting at 8.10 pm

Chairman's signature

Likely to contain exempt information under paragraph(s) 3 of
Part 1 of Schedule 12A of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

Likely to contain exempt information under paragraph(s) 3 of
Part 1 of Schedule 12A of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank