APPENDIX 2

Data Protection Policy

Item	Details
Reference:	Information Governance-1 DPP
Status:	Final
Originator:	Head of Legal & Support Services
Owner:	Data Protection Officer
Version No:	1:2
Date:	24 September 2024

Key policy details

Approvals

Item	Date of Approval	Version No.
Consulted with N/A		
Reviewed by Audit and Governance Committee	7 August 2024	1:1
Approved by Cabinet	24 September 2024	1:1
Consulted with Internal Audit	October 2025	1:2

The policy owner has the authority to make the following minor changes without approval.

- **Operational Changes** - any modification in data protection procedures or required alignments with other documents within the Information Governance Framework.
- **Regulatory Decisions** - when Court or regulatory decisions impact information security practices.
- **Legislation and Guidance Changes** - If there are changes in legislation or regulatory guidance related to data protection the policy owner should review and update this policy accordingly.

Policy Location

This policy can be found at NWLDC's website and the Sharepoint page under current policies tab.

Equality Impact Assessment (EIA)

Completed by	Completion date
Fay Ford	1 June 2024
Laurent Flinders	14 October 2025

Revision History

Version Control	Revision Date	Summary of Changes
1:1	July 2024	Creation of Document
1:2	October 2025	Update to include the Data (Use and Access) Act 2025 Implementation of CCTV and Surveillance Camera Technologies Update to the Data Protection Principles to include Accountability Update to Data Subject rights to include automated decision making

Policy Review Plans

This policy is subject to a scheduled review once every year or earlier if there is a change in legislation or local policy that requires it.

Distribution

Title	Date of Issue	Version No.
Distributed to Cabinet	24 September 2024	1:1
Published on NWLDC Website	27 September 2024	1:1

Data Protection Policy

1. Introduction

North West Leicestershire District Council ('the Council') has responsibilities under the Data Protection Act 2018(DPA 2018), UK General Data Protection Regulation (UK GDPR), Data (Use and Access) Act 2025 (DUAA), Local Government Acts and the Human Rights Act 1998 to protect rights of privacy and ensure that personal data is sufficiently protected when it is being processed.

The Council is required as part of its overall information governance structure to ensure that appropriate controls are implemented and maintained in the collection and use of personal information pertaining to its customers, clients and staff and that these are in accordance with the requirements of the current data protection law (the DPA 2018 and the UK GDPR along with other legislation).

In most cases the Council will be the data controller for the personal data it processes. A data controller is the organisation or person who determines and controls the purpose for the processing of personal data. In some cases, the Council may be a joint data controller with another organisation.

There may also be circumstances in which the Council has appointed a third party to process data on its behalf and in such circumstances that party will be a data processor but the Council will remain the data controller.

This policy sets out the Council's approach to complying with the above legislation in relation to data protection and forms part of the Council's Information Governance Framework, which applies to all staff including employees, councillors, agency staff, contractors, volunteers or any other persons who have access to, or use the Council's information concerning personal data.

2. Scope

This policy forms part of the Council's Information Governance Framework, which applies to all staff including employees, councillors, agency staff, contractors, volunteers or any other persons who have access to, or use the Council's information.

The scope of this policy requires compliance with the principles defined in law.

Personal data is defined as:

Any information related to an identified or identifiable living natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identifications number,

location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4 UK GDPR).

Special category personal data is defined as personal data relating to any of the following (Article 9 UK GDPR):

- Racial or ethnic origin.
- Political opinions.
- Religious or Philosophical beliefs.
- Trade Union membership.
- Genetic or biometric data for the purpose of uniquely identifying a natural person.
- Data concerning health.
- Sex life or sexual orientation.

Criminal Offence data is personal data relating to criminal convictions and offences or related security measures (Article 10 UK GDPR).

Section 10 of the Data Protection Act provides the framework for processing data relating to criminal convictions and offences.

Criminal offence data can only be processed:

- Under the control of official authority, or
- If authorised by domestic law - this means that one of the conditions in schedule 1 of the DPA is met.

All personal data must be protected. Special category personal data and criminal offence data may require special protection measures.

3. Principles of Good Practice

The UK GDPR includes seven key principles outlined in Article 5, which must be adhered to whenever personal data is processed. Processing includes obtaining, recording, using, holding, disclosing and deleting personal data.

All employees processing personal data must ensure they adhere to the principles as defined in the data protection law which require that personal data is:

- Used fairly lawfully and transparently.
- Used for specified, explicit and legitimate purposes.
- Used in a way that is adequate, relevant and limited to only what is necessary.
- Accurate and where necessary kept up to date.
- Kept for no longer than is necessary for the purposes for which it was collected.
- Handled in a way that ensures appropriate security including protection against unlawful or unauthorised processing, access, loss destruction or damage.
- Accountability- As a data controller the Council is responsible for complying with the above principles and must be able to demonstrate compliance.

4. Access and use of Personal Data

This policy applies to everyone that has access to personal data and includes any third party or individual who conducts work on behalf of North West Leicestershire District Council or who has access to personal data for which the council is responsible and who

will be required contractually or otherwise to comply with this policy.

The Policy is also applicable to Members who create records in their capacity as representatives of the Council.

It is an offence for any person to knowingly or recklessly obtain, procure or disclose personal data, without the permission of the data controller.

All data subjects are entitled to:

- Be informed about how data is being used.
- Access personal data.
- Have incorrect data updated.
- Have data erased.
- Stop or restrict the processing of data.
- Data portability (allow data subjects to get and reuse data for different services).
- Object to how data is being processed in certain circumstances.
- Not be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant effects.

The above rights are not absolute and only apply in certain circumstances

The Council will process all personal data in accordance with the relevant legislation. Where the Council is seeking to pursue a new project or process that involves the use of personal data, a data protection impact assessment will be carried out to assist the Council in systematically analysing, identifying and minimising the data protection risks.

The Council will only process personal data where it complies with the data protection principles under the legislation and in doing so will only process the minimum personal data required for the intended purpose. The Council will also seek to use anonymised data where appropriate to do so in order to avoid the retention of personal data where it is not necessary to retain it.

In the collection and retention of personal data, the Council will take reasonable steps to ensure that the personal data held is accurate, up-to-date and not misleading. All personal data will be retained in accordance with the Council's retention schedule.

The Council holds an information asset register, which includes information about data processing activities and any systems that process personal information.

Personal data will be processed and stored by the Council in accordance with the Council's IT Security Policy. Where the Council appoints a third party to process personal data on its behalf, it will enter into a data processing agreement with the third party to ensure that the personal data is sufficiently protected. The Council will ensure that information processed by third parties is done so in line with legal requirements and good practice.

The Council has privacy notices which explain why it collects personal data, how that personal data is used and shared (if applicable), and the rights that people have over their personal data.

5. Sharing Personal Data

There may be a need for the Council to share personal data that it holds with another

party, in which case it will only do so where it has a legal obligation, power or permission to do so. Where appropriate, individuals will be informed that their personal data is being shared and any personal data shared will be undertaken confidentially and securely.

The Council will ensure that data sharing agreements are in place (where appropriate) to set out the terms on which personal data will be shared with another party. The Council also maintains a register of data sharing arrangements.

Where personal data is being transferred, the Council will endeavour not to transfer personal data outside of the European Union, to third countries or international organisations unless there is a legal requirement to do so or it can be evidenced that appropriate safeguards are in place as required by data protection legislation. In the event that international transfers are being considered, a data protection impact assessment will be undertaken.

Personal data within the Council will only be accessed by those employees that need to access the information for their role and business need. There may be circumstances in which it is appropriate to limit access to certain personal data to specific members of staff, due to the sensitive nature of the personal data and/or how it is being used.

6. Information Security Incidents

The Council has a procedure for reporting, logging and investigating information security incidents. Where such information security incidents indicate that there has been a breach of data protection legislation, the Council will consider whether it is appropriate and necessary to report the breach to the Information Commissioner's Office in accordance with the Council's procedure.

All incidents of a personal data breach must be reported to the Data Protection Officer via the staff portal. As much information as possible should be provided and reported as soon as or within '24hrs' of the incident being identified.

An information security incident includes but is not restricted to the following:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware or software characteristics without the Council's knowledge.
- The unauthorised use of a system for the processing or storage of any data by any person.

7. CCTV and Surveillance Camera Technologies

Surveillance Cameras Systems are recognised as all forms of technology that are able to capture, record and process images of persons and/or other forms of personal data.

The Council has a Surveillance Camera Technologies Procedure that sets out the deployment, use and management of Surveillance Camera System to ensure that all legal, regulatory and ethical frameworks are compiled with.

This Policy in conjunction with the Surveillance Camera Technologies Procedure will ensure the key principles of surveillance are adhered to including, but not limited to:

- Surveillance must be necessary, proportionate and justified.
- Systems must have a defined purpose (e.g crime prevention, public safety)
- Data Protection Impact Assessments (DPIAs) must be completed before deployment and reviewed annually.
- Clear signage and public awareness for overt systems.

This Data Protection Policy and the Surveillance Camera Procedure shall apply to all forms of Surveillance Camera Technologies operated by the Council, including the following:

- CCTV
- Automatic Number Plate Recognition (ANPR)
- Body worn cameras.
- Unmanned aerial systems (UAS)
- Vehicle mounted CCTV systems
- Mobile CCTV systems
- Facial Recognition Systems
- CCTV algorithms/analytics

If the Council introduces, or seeks to introduce, new forms of surveillance technology that capture Personal Data but are not listed above, the provisions of this Data Protection Policy will apply, and the Council will consider whether this policy requires amendments to take account of the specifics of the new technology.

The operation of Surveillance Camera Systems will be undertaken with regards to the following legislation:

- Data Protection Act 2018 (DPA 2018)
- UK General Data Protection Regulation (UK GDPR)
- The Human Rights Act 1998
- The Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000 (FOIA)
- The Surveillance Camera Code of Practice under the Protection of Freedoms Act 2012 (Popham 2012)

A central register of all surveillance systems will be held by the Councils Data Protection Officer and IT Team Manager to oversee compliance.

Further Information

The Information Commissioner's Office (ICO) is the independent authority set up to monitor compliance with the Data Protection Act and General Data Protection Regulation. It also issues guidance and good practice notes. You can contact the ICO here Information Commissioner's Office (ICO).

The ICO can consider complaints about an organisations failure to comply with the Act and regulations following the initial reply from that organisation.