NORTH WEST LEICESTERSHIRE DISTRICT COUNCIL

POLICY DEVELOPMENT GROUP – 11 JANUARY 2017

Title of report	**ICT SERVICES UPDATE**
Contacts	Councillor Nick Rushton 01530 412059 nicholas.rushton@nwleicestershire.gov.uk Interim Director of Resources 01530 454833 andrew.hunkin@nwleicestershire.gov.uk Interim Head of Transformation 01530 454520 anita.onwuchekwa@nwleicestershire.gov.uk ICT Team Manager 01530 454716 sam.outama@nwleicestershire.gov.uk
Purpose of report	To provide the Policy Development Group with information and assurance on the Council's future ICT security arrangements.
Council Priorities	Value for Money
Implications: Financial/Staff Link to relevant CAT Risk Management Equalities Impact Screening Human Rights Transformational Government	 All costs associated with the Data Centre project have been fully accounted for as part of the ICT Road Map. There are no staffing implications. Not Applicable A risk register has been developed as part of the project management process and in accordance with the corporate governance structure N/A None Modernisation of the Council's ICT infrastructure to provide high availability, enhanced security and improved disaster recovery and business continuity arrangements.
Comments of Head of Paid Service	The report is satisfactory

Comments of Deputy Section 151 Officer	The report is satisfactory
Comments of Deputy Monitoring Officer	The report is satisfactory
Consultees	None
Background papers	Audit and Governance Committee minutes – 13 July 2016
Recommendations	**THAT POLICY DEVELOPMENT GROUP:** **NOTES AND COMMENTS ON THE ICT SECURITY ARRANGEMENTS AS SET OUT IN THIS REPORT**

1.0 BACKGROUND

1.1 The Audit and Governance Committee (13 July 2016) raised a concern on the arrangements the Council had or was putting in place for the security of its systems and data. In particular there was a concern if these arrangements involved the use of 'cloud technology'.

1.2 The matter was referred to the Policy Development Group for consideration.

2.0 UPDATE

2.1 The Council is embarking on a mordernisation of its ICT arrangements summarised in the ICT Road Map (appended). This will include improving the security of its systems and data by moving its servers (virtual and physical) and infrastructure away from the main Council offices, into a managed secure private data centre. In addition this will provide: improved disaster recovery and business continuity arrangements, higher availability, more secure backups, more secure access, scalability and cost savings.

2.2 A data centre is ideal for companies and organisations that need a customised, dedicated system that gives them full control over their data and equipment; and is extremely suitable for organizations that run many different types of applications and complex workloads. The underlying platform is managed by the data centre with logical and physical separation.

2.3 A procurement exercise is being run and officers are currently evaluating tender submissions from private data centre suppliers, with a view to award following consideration by Cabinet on 17 January 2017.

2.4 The advantages of moving to a secure private data centre are as follows:-

1. The platform is hosted within the company's own data centres with company-owned resources.
2. The Council owns the security of all internal data, the platform is managed by the data centre. Only authorised users of NWLDC have access to the data.

3. Increased security against data leaks for organisations that handle extremely confidential or sensitive data. Enterprise class security is employed to ensure data is secure at all levels. Anti-spoof, anti-sniff firewall technology isolates your virtual machines.
4. You can grow and shrink your systems as you need to when you need to and everything is automated so new resources are added right away. You can add and delete virtual servers and turn them on and off as you need them.
5. Data centres provide further assurance by providing safety from fires, power shortages, floods and other factors that may otherwise damage servers and core infrastructure.
6. Reduced ICT infrastructure and management costs.
7. Data breaches have increased year-over-year and there's no end in sight, with data regulations becoming stricter and penalties becoming more expensive. Data centre facilities are hardened against forced entry, unauthorised access, fire and natural disasters. They offer multiple layers of security including 24/7 onsite security, biometric and cardkey entry, cabinet and cage locks, and camera surveillance.
8. The more secure IT infrastructure creates additional peace of mind in the event of a natural disaster, power outage, or other unexpected event. Moving to a private Data centre can ensure that our servers, equipment and applications will remain available and operational if the unexpected happens.

2.5 Data centres that are used by public sector organisations should meet a minimum standard that is capable of delivering efficient, reliable and highly available services. Some of the standards that have been considered in the tender evaluation are:

Physical security

2.6 One aspect of data centres which is often implemented at a low standard in many public sector-built data centres and computer rooms is physical security. It is crucial to evaluate security controls on physical infrastructure and facilities which include:

1. Built to comply with ISO27001 Information Security Standards.

2. Comply with the Escrow Agreement, for the protection and security of data.

3. BS7799 compliant and at least tier 3 for physical security,

4. Comply with the Payment Card (PCI) Data Security standard.

5. Cyber essentials plus Certified.

6. Logs and operational audit trails are correct, secured and maintained for as long as the customer requires

7. Ensure an effective governance, risk and compliance process exists

8. Ensure network connection are secure with firewalls, intrusion detection and intrusion prevention technologies which the Council already has in place

9. Compliance with ISO/IEC 27017 [4] "Code of practice for information security controls".

Support for business continuity and disaster recovery capabilities

2.7 A number of data centres provide some level of internal resilience and fault tolerance and this is measured by a tier rating. However many existing public sector data centres are not of a sufficient standard to be considered capable of sustained continuous operation in the event of a disaster, major or otherwise. Ensuring ICT systems can support continuous business operation is an area of increasing concern. Any move to a new infrastructure must have disaster recovery capability built in from the outset.

Environmental controls

1. Certified to the **ISO14001** standard
2. PUE rating – 1.8 or less

2.8 Once the contract has been awarded a site visit will be arranged for key stakeholders to go to the data centre to see the services offered, security within the data centre and the location of our secured ICT Infrastructure.

2.9 The Council will keep the suitability of the arrangement under review through the yearly ICT internal and external audits which are conducted on our infrastructure, security and key controls - as well as the yearly IT health check which is conducted to attain Public Secure Network(PSN) certification and, more recently the Cyber essentials Plus government accreditation scheme.