NEWARK & SHERWOOD DISTRICT COUNCIL

Report to: Cabinet Meeting - 21 January 2025

Portfolio Holder: Councillor Paul Peacock, Strategy, Performance & Finance

Director Lead: Sanjiv Kohli, Deputy Chief Executive Director - Resources

Lead Officers: Dave Richardson, ICT & Digital Services Business Manager, Ext. 5405
Stacy Carter, Senior Information Governance and Data Protection Officer, Ext. 5216

Report Summary	
Type of Report	Open Report, Non-Key Decision
Report Title	Implementation of an Information Security Management System (ISMS)
Purpose of Report	To provide Cabinet with an understanding of implementation of an Information Security Management System (ISMS) for legal and regulatory compliance.
Recommendations	That Cabinet approve the Implementation of the ISMS for the Council.
Alternative Options Considered	Various alternative frameworks and the option to take no action have been evaluated. However, this international standard for information security is mandated by the Council for procuring systems and technology, where applicable.
Reason for Recommendations	To align with the community plan objective 8: To be a top performing, modern and accessible Council. Community trust in the Council to manage and use their data in a secure and compliant way, whilst demonstrating transparency.

1.0 Background

1.1 This report outlines the design and implementation of the Information Security Management System (ISMS) for the Council, following the ISO/IEC 27001:2022 standard. The purpose of the ISMS is to protect the Council's information assets from various threats, ensuring confidentiality, integrity, and availability.

1.2 The primary objective of the ISMS is to establish a framework that protects all council information assets, both physical and electronic, from internal and external threats. This framework complies with the ISO/IEC 27001:2022 standard and aligns with the Council's regulatory, operational, and contractual obligations.

1.3 The Corporate Information Governance Group (CIGG) is made up of Senior Leaders and Business Managers across the Council and are responsible for the effective management of Information Security and Information Governance risks across the Council and wholly owned companies. Therefore, the CIGG is responsible for managing the ISMS, ensuring that its implementation and maintenance are cohesive and effective. Work to date has been a collaborative effort, with multiple business units across the Council working together to design the ISMS with consideration to operational impact. The shared approach not only promotes a unified security posture but also ensures that the ISMS is tailored to meet the specific needs and challenges of the Council, thereby enhancing overall compliance and security.

1.4 Furthermore, within our supply chain and contractual agreements, we recommend and request ISO27001 certification as part of our due diligence process to ensure that suppliers safeguard the Council's data assets, therefore there is a reasonable expectation that the Councils works towards this standard.

1.5 Organisations implement ISO27001 to establish a robust Information Security Management System (ISMS) that safeguards its information assets against internal and external threats. This certification ensures compliance with regulatory, operational, and contractual obligations, enhances data confidentiality, integrity, and availability, and fosters a culture of security through regular risk assessments, asset management, access control, and incident response.

1.6 Additionally, it promotes trust within our communities as the custodians of their data. Furthermore, promotes stakeholder engagement, as employees, contractors, and external partners are educated and aligned on maintaining consistent information security practices, thereby reinforcing the Council's overall security posture and reputation.

1.7 In current times, the importance of ISO27001 certification is more pronounced than ever due to several evolving factors.

a) Firstly, the post-pandemic shift towards more digital systems has increased the volume and sensitivity of data being processed, necessitating enhanced security measures to protect against breaches.
b) Secondly, the rise in cyber threats, with hackers and malicious actors becoming more sophisticated, requires organisations to adopt comprehensive security frameworks like ISO27001 to safeguard their information assets.
c) Additionally, the complexity of modern work environments and the growing number of staff can inadvertently lead to data breaches, emphasising the need for stringent security protocols.
d) Lastly, the proliferation of remote working has expanded the attack surface, making it imperative for organisations to ensure robust security practices are in place to protect data accessed from various locations.

1.8 The successful implementation of an Information Security Management System means the Council is adhering to legislative, regulatory and third party data management requirements such as the ICO requirements, UK data privacy legislation and the Department of Work and Pensions Memorandum of Understanding (DWP MOU).

1.9 The ISMS framework encompasses several components, including risk assessment, asset management, access control, and incident response. Each of these components plays a crucial role in maintaining the security posture of the council's information systems. Risk assessments are conducted regularly to identify potential vulnerabilities and threats, allowing for timely mitigation measures. Asset management ensures that all information assets are accounted for and protected, while access control measures restrict unauthorised access to sensitive data.

1.10 Additionally, the ISMS includes a robust incident response plan that outlines procedures for detecting, reporting, and responding to security incidents. This plan ensures that any breaches are managed swiftly and effectively, minimising potential damage to the council's operations and reputation. Regular audits and reviews are also conducted to ensure continuous improvement and compliance with the ISO/IEC 27001:2022 standard.

1.11 The ISMS provides foundational support to new legislation, government changes and operational demands by ensuring a secure data management approach.

1.12 Next steps for the ISMS implementation

The next steps include:

a) Implement ISMS policies and track progress with action logs and non-conformity lists.
b) Expand the risk log and ensure all staff understand their security responsibilities.
c) Provide ongoing training programs to maintain staff awareness of ISMS policies.
d) Conduct internal audits to ensure compliance and identify improvement areas.
e) Establish a review process for continuous ISMS effectiveness and alignment with Council goals.

1.13 A policy map is included (**Appendix A**) that acts as a visual representation of policies, terms, roles and responsibilities, control sections and acknowledges supporting strategies and plans.

2.0 Proposal/Details of Options Considered

2.1 Approve the implementation of the Information Security Management System (ISMS) for the Council, with oversight by CIGG, to mitigate information security risks within our community.

2.2 Information & Communication Technology, security and information governance, systems and processes are fundamental to all activities of the Council. Without robust policies and controls, the Council would be unable to operate at the high standard that our communities now expect and deserve.

3.0 Implications

In writing this report and in putting forward recommendations, officers have considered the following implications: Data Protection; Digital & Cyber Security; Equality & Diversity; Financial; Human Resources; Human Rights; Legal; Safeguarding & Sustainability and where appropriate they have made reference to these implications and added suitable expert comment where appropriate.

3.1 Financial Implications

No financial implications in this report.

3.2 Human Resources Implications - HR2425/3117 SL

a) The implementation of the ISMS will give employees a consistent standard to work to and provide for a clear framework in which they can operate safely and with confidence.

b) Employees will need to be adequately trained, and it is noted that the implementation plan makes provision for training and cultural change over the 2-year period with some workshops, training programmes and courses provided in person and on the Ambition Academy e-learning platform.

c) We aim to foster a 'no blame' culture, and we would encourage staff to report any mistakes they make when handling data. However, failure to adhere to the new requirements may, in serious or repeated circumstances, lead to disciplinary action, and employees should be made aware of the impact this could have on their employment during training and in policy or procedural documents.

3.3 Legal Implications

Cabinet is the appropriate body to consider the content of this report. Successful implementation of ISMS will assist the Council in meeting its statutory data protection obligations.

Background Papers and Published Documents

Except for previously published documents, which will be available elsewhere, the documents listed here will be available for inspection in accordance with Section 100D of the Local Government Act 1972.

None.

Appendix A – ISMS Policy Map