Report to Cabinet

Subject: Annual Report on behalf of the Senior Information Risk Owner 2024/25

Date 9 October 2025

Author: Deputy Chief Executive

Wards Affected

Borough wide

Purpose

To present a report on behalf of the Senior Information Risk Owner providing an annual review of activities in respect of information management and data security.

To seek approval of the Identification and Verification Policy which provides guidance to officers on how customer's identification should be verified.

Key Decision

This is not a key decision.

Recommendation

THAT Cabinet:

1) Note the Annual Report on behalf of the Senior Information Risk Owner

2) Approve the Identification and Verification Policy at Appendix 2

1 Background

1.1 As Members are aware, Senior Leadership Team approved an Information Security Governance Framework setting out the Council's approach to information and cyber security risk which was endorsed by Cabinet on 1 August 2019.

1.2 The Council's designated Senior Information Risk Owner (SIRO), currently the Deputy Chief Executive and Monitoring Officer, has overall responsibility for the Council's information management framework and acts as the champion for information risk within the Council. The SIRO is currently

supported by the Data Protection Officer, Deputy Data Protection Officer, the Assistant Director for Digital, Data and Technology and the Cyber Compliance and Policy Manager. The SIRO is responsible for producing an Annual Report on information governance. The Annual Report has been prepared on behalf of the SIRO and is attached at Appendix 1. The report provides an overview of activity in relation to information governance, key achievements during 2024/25 as well as outlining work planned for 2025/26. It should provide assurance that the Council has arrangements in place to ensure information risks are being managed effectively.

1.3 It is important that the Council recognises the need to protect its information assets from both accidental and malicious loss and damage. The loss or damage of information can have serious consequences for the Council; not only financial and reputational but also may result in the Council being unable to deliver vital services to customers. As a result, Information Governance must be taken very seriously by the Council and this is evidenced by the on-going work activity to ensure the management and security of our information.

1.4 The Council has recently been audited by internal auditors in relation to its processes and procedures in relation to Information management. The auditors gave moderate assurance in relation to design and effectiveness with recommendations which have been included within the report and actioned in 2024/25. A significant amount of work has been undertaken including new GDPR training being rolled out across the Council and changes from Information Asset registers to Records of Processing Activity for each service area providing detail by department of what data is held and the legal basis for processing as well as information on retention, this work is ongoing.

1.5 Cabinet will recall that in March of last year the Council's Digital, Data and Technology Strategy was approved, in addition, there has been a senior management restructure with appointment of an Assistant Director for Digital, Data and Technology and a restructure of the Council's ICT team.

1.6 This investment in transformation and the recognition of its significance in driving the Council forward has to be supported by a solid governance framework in relation to ICT and data security. Work in 2024/25 was focused on strengthening cyber resilience and improving risk management in these areas. The establishment of the Business Design and Technology Authority, a body of officers that oversees requests for system changes and implementation has data security as one of its key principles when reviewing projects. In addition, the Corporate Risk Board now has oversight of Information Security and associated risks. Changes to the procurement process has also strengthened the engagement with ICT in respect of software contracts.

1.7 Work has also been underway to improve identification and verification processes at the Council. This ensures that personal data is disclosed to the right person with the right authorities and consents in place. An

Identification and Verification (IDV) Policy has been prepared in consultation with the Data Protection Officer to provide a consistent approach for checking customer identification. This is attached at Appendix 2.

2 Proposal

2.1 It is proposed that the Annual Report of the SIRO 2024/25 at Appendix 1 be noted.

2.2 It is proposed that Cabinet approve the IDV Policy at Appendix 2 in order to provide clarity for staff and customers in relation to how identification will be verified and ensure a consistent approach to disclosure.

3 Alternative Options

3.1 Not to present an annual SIRO report, in which case Executive members will not be updated on information governance activity across the Council and understand whether information risks are being managed effectively.

3.2 Not to have a consistent approach to IDV through a policy document, this does potentially increase the risk of disclosure of personal information to the wrong recipient.

4 Financial Implications

4.1 There are no financial implications directly arising from this report.

5 Legal Implications

5.1 The Council must comply with a number of statutory obligations in the General Data Protection Regulations, Data Protection Act, Freedom of Information Act and Environmental Information Regulations.

6 Equalities Implications

Appendix 3 – Equality Impact Assessment

7 Carbon Reduction/Environmental Sustainability Implications

There are no carbon reduction/environmental sustainability implications directly arising from this report.

8 Appendices

8.1 Appendix 1 – Annual report of the Senior Information Risk Officer 2024/25

Appendix 2 – Identification and Verification policy

Appendix 3 – Equality Impact Assessment

9 Background Papers

9.1 None identified.

10 Reasons for Recommendations

10.1 To ensure the Executive is updated in respect of the Information Governance activity across the Council in order to provide assurance that information risks are being managed effectively and to ensure Information Governance Policies are in place to mitigate risks.

Statutory Officer approval

Approved by the Deputy Chief Financial Officer
Date:

Drafted by the Monitoring Officer
Date: