Chelmsford City Council Governance Committee

18 November 2026

Information Governance Update

Report by:
Information Governance Manager & Data Protection Officer

Officer Contact:
John Breen, Information Governance Manager & DPO, email: john.breen@chelmsford.gov.uk, tel: 01245 606215

Purpose
To provide an annual update on the Council's approach to the assurance and management of information.

Recommendations
To note the contents of this report.

Summary of Key Points
1. Statutory request performance remained strong, with 93% compliance and no ICO referrals.
2. The Council continued to strengthen cyber security, information governance and staff awareness arrangements.
3. Significant progress has been made in records management, including the implementation of retention periods for Outlook and OneDrive and improvements to the Council's Record of Processing Activities.
4. Further work is planned to align with the Cyber Assessment Framework and continue improving information governance maturity.

1. Introduction

1.1. The purpose of this report is to provide an annual update on the Council's approach to the assurance and management of information.

2. Achievements and Further Developments

2.1. Statutory Requests - Information requests comprise Freedom of Information requests, Environmental Information Regulations requests and Data Protection Act Subject Access Requests. In 2024/25, the Information Governance Team, working with Council services, processed 979 requests, of which 93% were answered within the statutory timescale. In 2025/26, 997 requests were received and 93% were also answered within the statutory timescale. No cases relating to these requests were referred to the Information Commissioner's Office (ICO) during 2025/26. While request volumes continue to increase by only around 2-3% each year, requests are becoming increasingly complex and resource-intensive to administer.

2.2. Data Breaches - the number of personal data breaches recorded was 38 in 2023/24, 23 in 2024/25 and 30 in 2025/26. The 30 breaches recorded during 2025/26 are categorised as follows (with last year's figures in brackets):

- 17 email breaches (12) – including emails sent to the wrong recipient or the use of the 'To' field instead of 'Bcc', resulting in recipients being able to view each other's email addresses.
- 10 enveloping breaches (9) – where correspondence intended for different individuals is enclosed in the same envelope or sent to an incorrect address.
- 0 security breaches (0) – relating to cyber incidents, phishing attacks or other information security compromises.
- 3 other breaches (2) – errors involving the publication of documents online.

All data breaches are subject to investigation in accordance with the Council's Data Breach Procedure, with lessons learned used to reduce the risk of recurrence and strengthen information handling practices. No breaches were reported to the ICO during 2025/26, consistent with the position in 2024/25.

2.3. Cyber Security - Cyber security has remained a significant focus for the Council in recent years, with further improvements made during 2025/26. The CISO role continues to be undertaken by the Digital Services Manager. The Council has enhanced its cyber security monitoring and incident response capabilities through regional collaboration and specialist support. Working alongside other authorities has strengthened the Council's cyber security posture and enabled effective responses to emerging cyber threats. This collaborative approach has also helped maintain operational resilience and support preparations for Local Government Reorganisation. The Council has

continued to invest in its technical infrastructure, including new hardware, system upgrades and security patching. Progress has also been made in migrating services to hosted solutions, either through third-party providers or the Council's own Dynamics 365 platform. Like all councils, the Council has been advised to work towards the new Cyber Assessment Framework. Adoption of the Framework will help demonstrate the progress made in strengthening the Council's cyber resilience. However, implementation will require engagement from a range of services across the authority

2.4. Training and Awareness - The ‘human factor’ remains one of the most significant risks to information security. Ensuring that staff and Councillors are appropriately trained is therefore a key component of the Council’s data protection and cyber security framework. The Council has continued to deliver mandatory annual information governance and cyber security training and provides targeted awareness communications and guidance throughout the year to support good information handling practices. In November 2025, the Council launched its latest organisation-wide training programme, achieving a completion rate of 92%, an increase from 90% in the previous year. The Council will continue to promote awareness of data protection and cyber security risks and responsibilities across the organisation. Following the successful completion of the November 2025 training programme, the Council's training provider ceased delivering services to the Council in March 2026. The Council is therefore considering options for a replacement solution. Whilst previous considerations were influenced by the anticipated changes arising from Local Government Reorganisation, the Council recognises the importance of maintaining effective cyber security awareness arrangements over the medium to longer term and will review the most appropriate approach during 2026/27.

2.5. Consents - the General Data Protection Regulations (GDPR) introduced more stringent requirements around consent, requiring organisations to ensure that consent is obtained and recorded appropriately. During the year, the Council strengthened its approach through the use of granular preference lists and a double opt-in process, helping to ensure that marketing communications are targeted, compliant and based on clear subscriber choices. The Council has also reintroduced website sign-up pop-ups to support list growth while maintaining compliance. The Council's e-shot marketing platform now contains over 102,000 unique contacts, while the Theatre's separate marketing database contains almost 58,000 emailable subscribers. Engagement remains strong, with average email open rates exceeding industry benchmarks and unsubscribe rates remaining low.

2.6. Privacy Notices - organisations are required to have privacy notices to inform users how they are going to use their data before receiving it. The Council now has over 30 privacy notices in place across a range of different service areas, which are regularly reviewed and updated.

2.7. Risk Management - information governance risks have been developed and fit the Council's risk management criteria. They are an important step in the Council's maturing information governance framework and enable the Council to put more effort and resources into areas which carry a higher risk.

2.8. Data Protection Impact Assessments (DPIAs) - DPIAs are a valuable tool for helping organisations identify and minimise privacy risks when introducing new processes, technologies or ways of working. In certain circumstances, they are a statutory requirement under UK GDPR and are used by the Council where there is likely to be a high risk to individuals' rights and freedoms. During the last year, DPIAs have been completed across a range of service areas and projects, including the use of drones, the implementation of RotaCloud and the introduction of AI agents within leisure services. These assessments help ensure that privacy and data protection considerations are embedded into projects from the outset.

2.9. Policies - the Council has a number of policies relating to information governance, cyber security and the protection of personal information. During the last year, the Council reviewed its Marketing Policy to improve the way marketing consents are obtained and recorded, and introduced a new WhatsApp Policy to provide clearer controls and guidance on the appropriate use of messaging applications for Council business.

2.10. Council Records and Records Retention - Effective records management is essential to the efficient operation of the Council. As services continue to modernise the technology they use, opportunities arise to improve the management and retention of records. During the last year, significant progress has been made in reviewing and updating the Council's Records of Processing Activity (ROPA). As required by UK GDPR, the ROPA provides a clearer understanding of the personal information held by the Council, how that information is used and the retention periods that apply. This work will support improvements in records management, reduce the volume of information retained beyond business need and assist preparations for Local Government Reorganisation, where information assets from multiple authorities may ultimately need to be consolidated.

2.11. Over the last two years, a seven-year retention period for emails held in Microsoft Outlook and documents held in OneDrive has been successfully implemented across the organisation. In March 2027, the Council intends to reduce the retention period for Outlook emails and OneDrive documents to five years as part of its ongoing programme of records management and information lifecycle improvements.

3. Conclusion

3.1. The Council has continued to make positive progress during the last year and has achieved strong outcomes across a range of information governance and cyber

security disciplines. Nevertheless, the threat landscape and regulatory environment continue to evolve, requiring ongoing investment in technology, training and governance arrangements to maintain and strengthen existing standards.

List of appendices:

None

Background papers:

None

Corporate Implications

Corporate Implication	Response
Legal/Constitutional	These are set out in the report
Financial	None
Potential impact on climate change and the environment	None
Contribution toward achieving a net zero carbon position by 2030	None
Personnel	None
Risk Management	None
Equality and Diversity	None
Health and Safety	None
Digital	None
Other	None

Equality Impact Assessment Conclusion

No Equality Impact Assessment required as a standard report for noting.

Consultees:

None

Relevant Policies and Strategies:

These are set out in this report