Chelmsford City Council Governance Committee

15 October 2025

Information Governance Update

Report by:
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

1. To note the contents of this report.

Achievements and Further Developments

1. Statutory Requests – information requests comprise of Freedom of Information, Environmental Information Regulations and Data Protection Act Subject Access Requests. In 2024/25 the Information Governance Team, together with services, processed 979 requests and 93% were answered within statutory timescales. This compares with 934 requests received in 2023/24 where 93% were also answered within timescale. Additionally, one case relating to these information requests was referred to the Information Commissioner's Office (ICO) in 2024/25 and the ICO upheld the Council's decision.

2. Data Breaches – the number of data breaches reduced from 38 in 2023/24 to 23 in 2024/25. These breaches are categorised as following (with last year's data in brackets):

    i. 12 email breaches (24) – consists of officers putting email addresses in the 'To' field instead of 'Bcc' field enabling recipients to see each other's email addresses; or officers sending emails to the wrong recipient.
    ii. 9 enveloping breaches (11) – where two or more letters for different individuals are put in the same envelope or letters are sent to the wrong address.
    iii. 0 security breaches (1) – relates to cyber-attacks, phishing attempts etc.
    iv. 2 other breaches (2) – errors in online forms.

    All data breaches are investigated thoroughly in line with the Council's Data Breach Procedure. These investigations also enable the Council and officers a chance to learn from these breaches. In addition, no cases relating to data breaches were referred to the ICO in 2024/25, the same as in 2023/24.

3. Phishing - in August the Council ran phishing campaigns which invited employees and Councillors to click on links and enter in their Council email address and password. In the wider world these types of attacks continue to rise and become more sophisticated as time progresses. The simulation run by the Council was an imitation of a real attack to provide employees and Councillors with more awareness to help them recognise real malicious attacks. During the year, the Council also ran service specific phishing exercises to highlight threats which are specific to that industry.
    As with all phishing simulations the outcome of this campaign has been carefully considered and is used to inform further the Council's response (including training and awareness) to cyber security risks.

4. Training and Awareness – the 'human factor' is often the weakest link in information security and therefore ensuring staff and Councillors are appropriately trained is a very important element of compliance for data protection and cyber security. In 2018/19, general GDPR eLearning training was delivered to all computer-based staff and the Council now launches a new training exercise for all staff and Councillors on an annual basis. The most recent training course was aimed at education through storytelling and Cyber Police series two was released. The Council achieved a completion rate of 90% (down 2% on last year; up 7% on two years ago). Series three of Cyber Police will be launched to the organisation by the end of the year.

5. Cyber Security Review – cyber security work has been a significant focus for the Council in recent years and further improvements have been made. The Virtual Chief Information Security Officer (vCISO) contract has now been completed, and the CISO role is now held by the Digital Services Manager,

with support from the previous vCISO on an ad hoc basis. The Council has recently signed a new Security Operations Centre (SOC) contract, working with other authorities, which will enable Essex information security sharing. We have continued our technical advancements, including new hardware, upgrades and patching of major systems, and advanced in our journey towards hosted products (either third party or in our own Dynamics 365 platform). We are still focussing on cultural elements, and we have seen progress in this area by refocusing messaging on data protection using examples from individuals' personal lives as well as organisational scenarios. In addition, different kinds of cyber security training are being rolled out to the organisation, including "escape room" style training. There are also some more tabletop exercises scheduled for the next 12 months. It is also likely the Council will have another baseline review as we are working towards the new Cyber Assessment Framework, and this will reflect the progress the Council has made in recent years. We also continue to apply and be successful in receiving government grants for our cyber security plans.

6. Policies – the Council has several policies which link to security and the protection of personal information which have been developed and reviewed in recent years. In the last year the Council has reviewed its Social Media Policy, Photography and Filming Policy and created an Artificial Intelligence Policy.

7. Consents – the GDPR introduced more stringent rules around consents, meaning organisations were required to consider how the consents were obtained in order to determine if they were GDPR compliant. The Council has refined its marketing lists to ensure adequate consents under GDPR are in place and have worked on rebuilding its depleted marketing lists. Currently, the number of general subscribers is 77,497 and Theatres subscribers is 51,309, as the number of subscribers continues to increase each year.

8. 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.

9. 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. An example of this has been the Council investing more resources in cyber security training and initiatives. In addition, information governance risks have recently been updated to ensure they are relevant and fit for purpose.

10. Contracts - one of the most difficult areas for the Council is ensuring that external suppliers are contractually aware of their legal responsibilities when handling information on our behalf, including whether they are complying with

data protection law in delivering services for the Council. All contracts issued, including standard Terms and Conditions, Framework Call-off Contracts and Bespoke Contracts contain appropriate data protection clauses. Suppliers are required to agree to these terms during the Procurement process and confirm this upon signature of the contract. OneCouncil holds all contract records that result from sourcing processes dealt with by the Procurement Team direct or where services have provided notification of a new low-value contract. Smaller contracts may still be put in place, by services, outside of our processes but the majority of these are covered by our standard Terms and Conditions.

11. Records Retention – managing records effectively is essential to the efficient running of an organisation. Over time, service areas improve the technology they work with, which has a positive effect on the management of records. Earlier this year, the Council successfully introduced a seven-year retention period for emails held in Microsoft Outlook. Early next year, the Council is implementing a seven-year retention period for documents held in OneDrive. This is an important step to further reducing the amount of information the Council holds and will lead to further improvements in the retention of records.

List of Appendices

Nil

Background papers:

Nil

Corporate Implications

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

Consultees: None

Relevant Policies and Strategies:
These are set out in this report