Chelmsford City Council Governance Committee

16 October 2024

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 2023/24 the Information Governance Team, together with services, processed 934 requests and 93% were answered within statutory timescales. This compares with 874 requests received in 2022/23 where 90% were answered within timescale. Additionally, one case relating to these information requests was referred to the Information Commissioner's Office (ICO) and the ICO upheld the Council's decision.

2. Data Breaches – the number of data breaches increased from 35 in 2022/23 to 38 in 2023/24. These breaches are categorised as following (with last year's data in brackets):

    i. 24 email breaches (15) – consists of officers putting email addresses in the 'To' field instead of 'Bcc' field enabling individuals to see other individuals' email addresses, or officers sending emails to the wrong recipient.
    ii. 11 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. 1 security breaches (3) – a supplier security error which led to information appearing online. The issue was resolved shortly after.
    iv. 2 other breaches (6) – other incidents which include errors in online forms and external reports.

    All data breaches are investigated thoroughly in line with the Council's Data Breach Procedure. These investigations also provide the Council and officers with an opportunity to learn from the breaches. In addition, no cases relating to data breaches were referred to the ICO in 2023/24, the same as in 2022/23.

3. Phishing - in April the Council ran a phishing campaign which targeted employees for personal information. 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 with more awareness to help them recognise real malicious attacks. 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 one was released to staff. The Council achieved a completion rate of 92% (up 9% from the training released the year before). Shortly, series two of Cyber Police will be launched to the organisation.

5. Cyber Security Review – once again cyber security work has been a significant focus for the Council and further improvements have been made. The Council's vCISO (virtual chief information security officer) service has been effective as we are working towards the new Cyber Assessment

Framework. Different kinds of cyber security training are being rolled out to the organisation, including “escape room” style training. We have also continued our technical advancements, including new hardware, upgrades (rollout of Windows 11) and patching of major systems, and continuing our journey to hosted products (either 3rd party or in our own dynamics 365 platform). The Council is still focussed 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. There are also some more tabletop exercises scheduled for the next 12 months. We also continue to apply and be successful in receiving government grants for our cyber security plans.

6. Policies – the Council have a number of 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 suite of policies including the Information Governance Policy, Data Breach Policy, Social Media Policy and Information Security Code of Conduct.

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. The number of subscribers across GovDelivery [general marketing] and Dotdigital/Spektrix [Theatres marketing] is now over 77,000 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 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 revised 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.

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 the standard Terms and Conditions, contain appropriate data protection clauses. Suppliers are required to agree to these terms before we purchase from them. OneCouncil now holds all contract records that result from sourcing processes dealt with by the Procurement Team. 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. To assist with the management of records, many authorities have introduced an email retention period in Microsoft Outlook. Management Team have recently agreed a retention period of seven years for emails stored in Outlook which becomes effective on 1st February 2025. This is an important step to reducing the amount of information an organisation 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