Chelmsford City Council Governance Committee

18 October 2023

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 2022/23 the Information Governance Team, together with services, processed 874 requests and 90% were answered within statutory timescales. This compares with 785 requests received in 2021/22 where 90% were also answered within timescale. Additionally, no [zero] cases relating to these information requests were referred to the Information Commissioner's Office (ICO) in 2022/23.

2. Data Breaches – the number of data breaches increased from 27 in 2021/22 to 35 in 2022/23. These breaches are categorised as following:

i. 15 email breaches – 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 – where two or more letters for different individuals are put in the same envelope or letters are sent to the wrong address.
iii. 9 other breaches – other incidents including 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 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 2022/23.

3. In July, 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. In 2018/19, general GDPR eLearning training was delivered to all computer-based staff. A year later a new eLearning course was launched and focussed on cyber awareness. In 2021/22, a new eLearning course on cyber awareness and home working was developed to coincide with the organisational shift towards more individuals working from home. The Council achieved a completion rate of 90%. Last year, the Council focussed again on cyber awareness and phishing, however the completion rate dropped to 83%. Cyber awareness training for this year is due to be released shortly.

5. Cyber Security Review – This year has been another year of intense work on Cyber Security, we have completed our first full year with the vCISO and this has proven to be a successful engagement as we align ourselves to industry best practice. The vCISO has met with a number of senior staff and we have made several updates to our policies and practices. There have also been many technical changes; migrating off existing third-party anti-virus to Microsoft’s Defender (which is included in our Office 365 license), replacing old firewalls with new Open Source based firewalls, and working on building our own single pane of glass cyber security alerts dashboard. These changes have allowed us to have much better visibility of our cyber security hygiene within our IT estate. Our technical controls have again been recognised as

being very strong, recently completing our PSN code of connection and for the first time not having any remediation work to do.

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 have developed House Rules for Social Media, and Consultation and Engagement Best Practice for Personal Sensitive Information. A review of our current suite of security and governance polices (including the Information Security Code of Conduct within the constitution) will take place within the next year.

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 74,000 as the number of subscribers increased by nearly 14,000 last 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 29 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. Data Protection Impact Assessments (DPIAs) – DPIAs are useful in helping organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. They are a statutory requirement in certain situations under GDPR and are used by the

Council when there is a significant change in the way personal data is processed, such as the purchase of a new IT system. Post GDPR, Management Team approved DPIA guidance for the Council and since then over 50 DPIAs have been completed across a wide range of Council services.

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
