Corporate Governance and Standards Committee Report

Ward(s) affected: n/a

Report of Joint Strategic Director, Transformation and Governance

Author: Ciaran Ward

Tel: 01483 444072

Email: ciaran.ward@guildford.gov.uk

Lead Councillor responsible: Joss Bigmore

Tel: 07974 979369

Email: joss.bigmore@guildford.gov.uk

Date: 6 October 2022

Data Protection and Information Security Update Report

Executive Summary

The transactions and interactions customers, residents and staff make with the Council often involve the sharing of personal data, for example in relation to council tax accounts, housing agreements, employment contracts.
It is therefore important that this data is used only in ways reasonably expected, and that it stays safe. Similarly, the secure collection, storage and transfer must be executed with regard to sound cybersecurity practices.

Recommendation to Committee

To note this report and approve the proposal for the report to be presented on an annual basis going forward.

Reason for Recommendation:

To ensure that the Committee is kept up to date with developments in the Council's data protection and information security framework.

Is the report (or part of it) exempt from publication? No.

1. Background

1.1 It is now over four years since the General Data Protection Regulation came into force. Various positive advances have taken place within the Council since then.

1.2 This report will cover developments in data protection and information security within the Council since the last report to this Committee in April 2022.

2. Update on Progress

Information Governance Successes since April 2022

- Further work completed with Waverley Borough Council's Data Protection Officer on data compliance requirements, including data sharing, as part of the Inter Authority Agreement associated with the Guildford and Waverley collaboration.

- ICT Refresh programme – 45% of systems now migrated off targeted legacy hardware and operating systems.

- Multi-Factor Authentication (MFA) - 79% of non-MFA users now migrated onto multi-factor authentication (more secure login technology).

- FOI performance figures continue to attain set target levels.

- Proposed migration of FOI logging system from eCase to Salesforce – now cancelled following decision to retain eCase as the most suitable system for recording of information governance requests.

- Homes for Ukraine scheme privacy statement finalised and now live on website to enable local homeowners to accommodate Ukrainian refugees

- Review of FOI hub co-ordinators/drafters across services has been completed and updated to reflect recent structural and organisational changes.

- Staff training on dealing with FOI/EIR requests on eCase system has been rolled out across service areas on a bespoke basis.

- Consent form for photography, filming and recording updated to encompass changes in practice.

- Continued advice and guidance given to staff on clear-out and deletion of redundant electronic and paper documents to ensure GDPR compliance and to save storage space.

Objectives for the next 6 months:

- Updating of policies/procedures – Covert Surveillance (Regulation of Investigatory Powers) Policy, Records Retention, Data Breach Response & Notification reporting Procedure to be reviewed and amended in consultation with relevant stakeholders.

- Multi-Factor Authentication (MFA) - Complete rollout of MFA to remaining Officers.

- Review of current Egress/email classification system.

- ICT Refresh Programme - Complete removal of legacy operating systems.

- Release of Council wide Cyber Security Awareness Training for all staff and councillors (provided by National Cyber Security Centre).

- Staff guidance on effective use of Microsoft Teams/Sharepoint to be finalised and published on intranet.

3. Data Breaches

3.1 There were 20 data breaches in 2021-22. Due to the small numbers of data subjects involved and the non-sensitive nature of the data in all cases, the Council decided to resolve the matter internally rather than notify the Information Commissioner's Office (ICO).

3.2 The most common type of breach involved emails or letters being sent in error to the wrong individual who usually had a similar name or address as the intended recipient; or in the case of emails sent to multiple recipients - addresses being typed into the CC field rather than the BCC field. In each case, a letter of apology was sent to the affected data subjects and measures were taken internally to prevent recurrence. None of the affected individuals decided to take matters further. Where appropriate, employees were briefed and, if necessary, given additional data protection training.

4. Equality and Diversity Implications

4.1 No Equality and Diversity Implications apply to this report.

5. Financial Implications

5.1 The Information Commissioner can issue a monetary penalty for failing to comply with the UK GDPR/Data Protection Act 2018. The range of fines can vary depending on the severity of the breach. In 2019 for example one local authority, the London Borough of Newham was fined £145,000 for negligently disclosing the names of over 200 people who appeared on a police database. In 2017 Gloucester City Council was fined £100,000 after 30,000 emails containing sensitive details were downloaded following a cyber-attack. The Information Commissioner found the council did not have sufficient processes in place to make sure its systems had been updated while changes to suppliers were made.

6. Legal Implications

6.1 Failure to handle information correctly or not having the appropriate security measures in place could potentially lead to breach of the legislation and possibly financial and reputational damage to the Council in the form of a monetary fine from the ICO as well as distress to any individuals affected by such incidents. There are therefore direct legal implications including the risk of reputational damage to the Council, adverse publicity and active monitoring by the ICO.

7. Human Resource Implications

7.1 There are no proposals in this report with any direct HR implications.

8. Future Reports

8.1 It is proposed that going forward this report is presented on an annual (rather than six-monthly) basis to cover the financial year period from April to March.

9. Background Papers

None

10. Appendices

None