Guildford Borough Council

Report to: Corporate Governance and Standards Committee
Date: 28 September 2023
Ward(s) affected: Not applicable
Report of Director: Transformation & Governance
Author: Ciaran Ward, Information Governance Officer
Tel: 01483 444072
Email: ciaran.ward@guildford.gov.uk
Lead Councillor responsible: Merel Rehorst-Smith
Tel: 01483 610581
Email: merel.rehorst-smith@guildford.gov.uk
Report Status: Open

Data Protection and Information Security Update

1. Executive Summary

1.1 The transactions and interactions customers, residents and staff make with the Council often involves the sharing of personal data e.g., in relation to council tax accounts, housing agreements, employment contracts.

1.2 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 of data must be executed with regard to sound information security practices.

2. Recommendation to Committee

2.1 That the Committee notes this report.

3. Reason for recommendation

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

4. Exemption from publication

No

5. Purpose of Report

5.1 To update developments which have occurred since the last report which was presented to Committee on 6 October 2022.

6. Strategic Priorities

6.1 To ensure adequate compliance with data protection and cybersecurity requirements, and to minimise risks.

7. Background

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

8. Update on Progress – Information governance developments since October 2022

- ICT Refresh programme – 54% of systems now migrated off targeted legacy hardware and operating systems.

- Public Sector Network (PSN) IT Health Check - ICT continues to work with Procurement to arrange a PSN compliant IT Health Check (including Penetration Test)

- Further work completed with Waverley Borough Council's Data Protection Officer on data compliance requirements, including –

    - Updated data sharing agreement (June 2023) to cover access to leaver accounts, as part of the Inter Authority Agreement associated with the Guildford/Waverley collaboration.
    - Shared GBC/WBC council tax statement on both councils' website which has led to increased efficiency in dealing with FOI/subject access requests concerning non-payment of council tax.
    - Shared Homes for Ukraine scheme privacy notice

- Data Breach Response & Notification reporting Procedure has been reviewed and updated to contain more user-friendly language, extended glossary and updates to changes both within GBC's internal structure and the wider legal and regulatory landscape – full text now live on intranet.

- Multi-Factor Authentication (MFA) for device log-in now rolled out to council officers and councillors.

- Working on joint project with WBC to update Covert Surveillance/ Regulation of Investigatory Powers (RIPA) Policy – to produce a common policy for both councils in order to ensure consistency in reporting, monitoring and approval of covert surveillance and acquisition of communications data. The draft policy was presented to this Committee at its last meeting. The Executive formally adopted the policy at its meeting on 24 August 2023.

- Information Governance Audit – Information Governance Officer is liaising with the Council's internal auditors – to be completed September 2023.

- Memorandum of Understanding with the Department for Work & Pensions for the purposes of data sharing with regard to certain council services

- Further all-staff emails have been sent out to warn staff of phishing scams from suspected cyber-criminals following a spate of fraudulent emails claiming to be from GBC's ICT team and sent to various employees advising them they needed to change their password.

- A new Cyber Resilience Programme has started, funded by a grant from the Department for Levelling Up, Housing and Communities (DLUHC). This seeks to improve the Council's cyber security through deliverables agreed with DLUHC.

- As part of the new councillor induction programme, councillors attended data protection and freedom of information training in June 2023.

9. Objectives for next 12 months

- Managing external and internal security penetration tests of council-wide systems – to work with Procurement to choose IT Health Check (security scans) provider for next scan.

- Updating of policies/procedures – Covert Surveillance (Regulation of Investigatory Powers) Policy, Records Retention Schedule, to be reviewed and amended in consultation with relevant stakeholders.

- Review of current Egress/email classification system.

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

10. Data Breaches

10.1 There were 16 data breaches in 2022-23. 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).

10.2 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.

11. Key Risks

11.1 Legacy hardware and operating systems are not being removed at the pace we would like – extended support arrangements are being considered.

11.2 There is a current vacancy for an Information Assurance Officer role that is crucial to supporting this area of work in the council. Unfortunately, so far recruitment has been unsuccessful. This poses a risk to the capacity available to support the work laid out in this report.

11.3 The volume of priorities being placed on ICT which far outweigh the resource available creates a capacity risk to undertake non-essential activities that support information governance.

12. Financial Implications

12.1 The ICO 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, 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.

13. Legal Implications

13.1 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.

14. Human Resource Implications

14.1 Not applicable.

15. Equality and Diversity Implications

15.1 Not applicable.

16. Climate Change/Sustainability Implications

16.1 Not applicable.

17. Summary of Options

17.1 Not applicable.

18. Conclusion

18.1 The Council will maintain best compliance with data protection and information security requirements through continued training of staff and councillors, appropriate technical measures and regular reviewing of the relevant policies and procedures.

19. Background Papers

None

20. Appendices

None