# Guildford Borough Council

Report to: Corporate Governance and Standards Committee
Date: 26 September 2024
Ward(s) affected: Not applicable
Report of Director: Legal & Democratic Services
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

# Annual Data Protection and Information Security Report

## 1. Executive Summary

1.1 The transactions and interactions customers, residents and staff make with the Council often involve the sharing of personal data e.g., 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 of data must be executed with regard to sound information security practices.

1.2 An annual report is provided to ensure that the Committee remains up to date with the Council's data protection and information security framework. The report sets out any changes or risks that have emerged during the previous year and objectives for the coming year.

## 2. Recommendation to Committee

2.1 That the Committee notes this report.

2.2 That future reports are separated so that there is an annual report on data protection and an annual report on information security.

## 3. Reason for recommendation

3.1 The Data Protection Officer (Information Governance Officer) and the Information Assurance Officer sit in different directorates as a result of reorganisation within the Council and it is therefore no longer appropriate to have a single report covering these areas. It will support good governance to have reports which focus on the separate and distinct areas and ensure sufficient consideration is given to both.

3.2 To recognise that the Committee has reviewed the developments that have occurred since the last report was presented on 28 September 2023 and ensure that the Committee remains aware of the Council's data protection and information security framework.

## 4. Exemption from publication

No

## 5. Purpose of Report

5.1 To set out the details of any developments which have occurred since the last report which was presented to Committee on 28 September 2023 and identify key areas for the coming year.

## 6. Strategic Priorities

6.1 To be a resilient and well managed Council by minimising risks and ensuring compliance with data protection and cybersecurity requirements.

## 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 September 2023.

## 8. Update on Progress – information governance developments since October 2023

- ICT Refresh Programme
    - All business system migrations have been completed.
    - The decommission of our older network is likely to take place in October as it is dependent on phone system changes that are being arranged with third parties.
    - Recent changes to financial controls as part of the new Constitution mean the remaining chargeable scope items for this programme are currently on hold. Approval from the Executive will be sought to enable the remaining programme budget to be used to deliver these.

- Cyber Resilience Programme
    - 9 of the 20 deliverables in this programme have now been completed.
    - ICT resource contention has significantly delayed this programme to date. Whilst resource contention will remain, as ICT continues to deliver without project resources, it is hoped that progress will improve once the ICT Refresh Programme is complete.
    - Recent changes to financial controls as part of the new Constitution mean the remaining chargeable scope items for this programme are currently on hold. Approval from the Executive will be sought to enable the programme budget (a grant) to be used to deliver these.

- The Public Sector Network (PSN) IT Health Check (effectively an internal and external security check) was completed in July. The ICT team is working to rectify higher-risk findings from this health

check.

- The Council's connection to the Public Sector Network (PSN) has been migrated to an alternative provider.

- The Council's office network connections have been largely migrated to a new solution. This follows the termination of Surrey County Council's UNICORN agreement with BT in August 2024. The replacement connectivity has reduced remote office technical dependence on Millmead House (improving resilience).

- The Council has begun replacing Egress (the Council's former secure email provider) with email encryption and Microsoft 365 "protected messages". Licences have already been reduced from around 700 to 400.

- New Information Assurance Officer specialising in cybersecurity matters appointed in April 2024.

- The Information Assurance Officer has run cybersecurity awareness training sessions for many higher-risk staff groups. This includes Customer Service agents, accountants, payroll staff etc.

- Further all-staff emails have been sent out to maintain staff awareness of phishing scams following a spate of fraudulent emails claiming to be from the Council targeting some staff members with malicious Internet links.

- Further work completed with Waverley Borough Council's Data Protection Officer on data sharing/compliance requirements, including:
  - Update of existing data sharing agreement currently in progress
  - Staff surveys being sent out

- Information Governance Audit – completed September 2023.

- Covert Surveillance & Investigative Powers Policy updated in September 2023 and published on the GBC intranet. Training for Authorising Officers and Investigatory/Enforcement Officers took place in July and September 2023 and further training is scheduled for October 2024 to ensure continuing compliance.

## 9. Objectives for next 12 months

- Completion of the ICT Refresh Programme (subject to Executive approval of budget).

- Continued delivery of projects within the Cyber Resilience Programme (subject to Executive approval of grant-based budget).

- Continued migration of staff from the Egress platform for secure email delivery.

- Implementation of changes to account authentication protection to align with good industry practice. This includes ceasing to expire passwords on standard accounts, and an update to our password length requirement.

- Further roll-out of Cyber awareness training.

- Update ICT policies to align with ISO/IEC 27001:2022.

- Replace the current public wi-fi solution to better reflect legislative requirements and wider availability.

- Risk Management Strategy to be updated

## 10. Data Breaches

10.1 There were 18 data breaches in 2023-24. For all but one case, due to the small number of data subjects involved, the non-sensitive nature of the data and the fact that the situation was under control, the Council decided to resolve the matter internally rather than notify the Information Commissioner's Office (ICO).

10.2 In relation to the single case, which was reported to the ICO, once the breach was discovered the compromised information was adequately contained and the situation was swiftly brought under control. The breach resulted from a disregard of our policies by a former member of staff and remains under investigation by the ICO. The Council has co-operated fully with the ICO in the investigation and if any recommendations are made as a result, they will be implemented.

10.3 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 minimise the chance of recurrence. None of the affected individuals decided to take matters further. Where appropriate, employees were briefed and, if necessary, given additional data protection training with a focus being made on encouraging all staff to become more vigilant and update their training.

## 11. Key Risks

11.1 Legacy hardware and software are not being removed at the pace we would like.

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

11.3 There is a risk of further data breaches which is being mitigated by regular training and increasing staff knowledge and understanding. Data breaches are monitored on a monthly basis and any trends are noted so that action can be put in place to reduce future breaches.

## 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 and can be significant depending on the nature and circumstances of the breach. Regularly reviewing policies, procedures and operating systems helps to reduce the risk of future breaches.

## 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, 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 There are sustainability implications associated with the disposal of legacy hardware, and energy use associated with new hardware and greater energy efficiency associated with increased cloud hosting.

These implications are kept under review as part of any changes being considered.

## 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