Redacted

REDACTED FINAL INTERNAL AUDIT REPORT

PERSONAL DATA BREACHES

CORP/01/2023

2 October 2023

Auditor	Trainee Auditor
Reviewer	Head of Audit and Assurance

Distribution list

Director of Corporate Services and Governance
Assistant Director & SIRO, IT
Head of Information Management

Executive Summary

Audit Objective	The objective of this audit was to assess the Council's response to personal data breaches in line with the Data Protection Act 2018 and to ensure that lessons are learnt from incidents to prevent reoccurrence.

Assurance Level		**Findings by Priority Rating**		
Reasonable Assurance	There is generally a sound system of control in place but there are weaknesses which put some of the service or system objectives at risk. Management attention is required.	**Priority 1**	**Priority 2**	**Priority 3**
		0	2	1

Key Findings

We found the following areas where controls are in place and working well:

1. Our analysis of the data breach incident log identified that a recurrent theme of personal data breaches is errors with emails, including emails sent to the wrong recipient. Although the risk of human error can never be eliminated, the Information Management Team evidenced that they have an action in progress to reduce the likelihood of email error by implementing an additional technical measure.
2. Appropriate information on reporting data breaches is readily available to staff via the intranet and the Council's policies align with legislation and Information Commissioner's Office (ICO) guidance.
3. For the cases that we sampled, we found through discussions with officers and review of documentation that there was an appropriate rationale for decisions not to report breaches to the data subject and / or the ICO.
4. 5/8 relevant cases had been reported to the ICO with the statutory 72 hour timeframe. There was a reasonable explanation for one exception and the other two are discussed in Recommendation 1 below.

We would like to draw managers' attention to the key findings below:

5. **Strategic oversight and lessons learned** (Priority 2) – There is currently limited corporate oversight and ownership of personal data breaches, to ensure that actions are implemented and lessons learned across the organisation. For 3/6 cases sampled, there was no evidence that actions to prevent reoccurrence had been taken within individual departments. ***See Recommendation 1.***
6. **Data breach records and investigations** (Priority 2) – Records of data breaches held by the Information Management Team were incomplete and, in some cases, inaccurate as, for example, five cases reported to the ICO or data subject had not been recorded as such on the central log. ***See Recommendation 2.***

We raised one further Priority 3 recommendation for good practice.

Management has agreed actions for all findings raised in this report. **Please see Appendix A**.

*Definitions of our assurance opinions and priority ratings are in **Appendix B**.*
*The scope of our audit is set out in **Appendix C**.*

Appendix A - Management Action Plan

1. Strategic Oversight and Lessons Learned	
Finding We understand that the Information Governance sub-group previously had oversight of personal data breaches, however this group no longer exists and there is no alternative body that receives regular assurance on the management of personal data breaches and lessons learned. Reporting to Corporate Leadership Team on Information Governance covers Freedom of Information and Subject Access Requests but does not cover data breaches. Whilst we acknowledge that there have been some organisation-wide communications on data breaches, there is no Council-wide group which oversees and scrutinises personal data breaches, disseminates lessons learned across the organisation and ensures that there is sufficient awareness of the Council's collective responsibilities within individual departments. For 3/6 cases that we sampled, there was no evidence to support that lessons learned had been identified and actioned within the relevant service (although we recognise that centrally, the Information Management Team are working on a solution to reduce the likelihood of human error with emails). We also found cases where officers within the relevant service had not notified the Information Management Team of the incident within 24 hours. One of these cases met the threshold for reporting to the ICO and consequently was not reported within the statutory 72 hour time period. A second case was reported late to the ICO because the relevant contractor did not immediately notify the Council that its data was affected as part of a wider incident. **Risk** Insufficient oversight may mean that effective management of data breaches is not embedded within individual services or the Council's culture, leading to avoidable errors or the Council not meeting its statutory obligations. The Council may incur significant financial penalties if relevant incidents are not reported to the ICO within statutory timeframes.	
Recommendation There should be appropriate corporate oversight and ownership of personal data breaches to: • ensure that appropriate actions are taken to prevent repeat occurrences • ensure that the Council meets its statutory obligations	**Rating** Priority 2

• cascade and disseminate lessons learned and issues arising within departments • raise awareness, and ensure compliance, within individual departments regarding the need to report breaches immediately to the Information Management Team, both to mitigate risk and to ensure the Council can meet statutory reporting timescales where relevant.	
Management Response and Accountable Manager (1) As part of the D&IT restructure and new IT managed service contract governance boards have been identified and will be implemented to include the discussion of data breaches and share lessons learned. (2) Breaches of significance are relayed to senior members of a directorate who may be involved in initial conversations or copied in to emails for information. This will be captured in breach logs and breaches of significance will be to the Senior Management Board. (3) Awareness will be raised at CLT and Managers briefing for officers to follow breach reporting guidance in an effort to ensure the Council meets the 72 hour reporting timescale where necessary, in line with recommendations. Accountable Manager: Head of Information Management	**Agreed timescale** (1) Jan-March 2024 in alignment with IT service provider contract implementation (2) 31st October 2023 (3) 30th November 2023

2. Data breach records and investigations
Finding The UK Data Protection Act 2018 states that organisations must keep records of personal data breaches including the facts relating to the breach, its effects and any remedial action taken. Our review of the Information Management Team's data breach Incident Log and sample testing of individual data breaches identified that the central records held were not fully complete, either because fields on the Incident Log had not been completed or because supporting documents were not readily available. This includes key errors in the information held such as: • one incident reported to the ICO which was recorded as 'not reported to the ICO' on the log • four incidents reported to the data subject which were recorded as 'not reported to the data subject' on the log

Further, the Council's Data Breach Investigation Guidance states that:

'Once an information security breach has been reported a member of the Information Management team will be identified to carry out the investigation and advise upon further action to, contain, remediate and recover if required. A manager or senior member of staff may be engaged within the service area to help during the investigation and offer further assistance if required to create a remediation action plan. The investigation should focus on what lessons can be learnt from the breach and what steps should be put in place to prevent a reoccurrence of the breach.'

There is template to complete for data breach investigations. This is dated 2018 although the Head of Information Management advised that it remains fit for purpose.

We found however that for 5/6 cases sampled for this purpose, the investigation template had not been completed. We also observed other cases during the course of our fieldwork where the template had not been completed or had not been fully completed.

Risk

Non compliance with the Data Protection Act 2018.
Ineffective oversight and management of personal data breaches, if information is not complete.
The investigation and outcomes do not cover all key aspects, actions are not identified and addressed, or decision-making cannot be subsequently justified.

Recommendation	**Rating**
Review end to end to process to ensure that information can be captured efficiently and effectively. Design and implement a proportionate quality assurance programme to ensure that records are accurate and up to date, and that necessary actions have been identified and completed.	Priority 2
Management Response and Accountable Manager	**Agreed timescale**
The process of logging the breaches with all necessary information to ensure all relevant information is recorded centrally will be reviewed and improved in line with recommendation. Accountable Manager: Head of Information Management	31st October 2023

3. Risk analysis and decision making	
Finding The Council's Information Security Policy and Data Breach Investigation Guidance do not specify that data breaches must be reported to the ICO within 72 hours, although we recognise that this requirement is clearly stated on the relevant intranet page. The policies also do not set out how a risk analysis should be undertaken in order to make a decision whether to report to the ICO or the data subject (including the risk factors to consider), and do not clarify who should make the decision to report or not. We were advised that the decision maker is the Head of Information Management or the Assistant Director – IT, but in practice, where the decision had been made not to report, this was made by a more junior officer within the Information Management Team. ICO guidance states that if a decision is made not to report a breach to the data subject, the organisation should ensure that the decision is documented. Whilst we were able to establish an appropriate rationale not to report for all cases sampled through discussions with staff and review of emails, our testing identified that the decision, and the risk-basis for the decision, was not always clearly or consistently documented. **Risk** Inappropriate decisions may be made, resulting in reputational damage or penalties from the ICO.	
Recommendation Review the suite of policies to enhance existing information concerning reporting to the ICO and the data subject, including timescales, risk analysis, documentation of risk analysis and decision making. The Data Breach Investigation Template could be amended to incorporate decision making for reporting purposes.	**Rating** Priority 3
Management Response and Accountable Manager There are clear breaches that do not meet the threshold to report based on information reported at the time and the initial risk assessment. The Principal Information Assurance Officer is deemed appropriate to determine where there is a clear need to not report to the ICO i.e. in such cases where there is clear containment of an incident, or the risk of identification is either mitigated or null. In all cases the Head of Information Management is sighted on the incident and will challenge if necessary.	**Agreed timescale** 30th November 2023

Where there is less clarity, or further considerations on reporting threshold and risk is necessary the Principal Information Assurance Officer will refer to the Head of Information Management for a decision. Where there is identification of potential significant risk to reputation and or financial penalty to the Council, the Head of Information Management will consult with the Data Protection Officer. The process and policies will be reviewed in line with recommendation and improved where necessary.	

Appendix B - Assurance and Priority Ratings

Assurance Levels

Assurance Level	Definition
Substantial Assurance	There is a sound system of control in place to achieve the service or system objectives. Risks are being managed effectively and any issues identified are minor in nature.
Reasonable Assurance	There is generally a sound system of control in place but there are weaknesses which put some of the service or system objectives at risk. Management attention is required.
Limited Assurance	There are significant control weaknesses which put the service or system objectives at risk. If unresolved these may result in error, abuse, loss or reputational damage and therefore require urgent management attention.
No Assurance	There are major weaknesses in the control environment. The service or system is exposed to the risk of significant error, abuse, loss or reputational damage. Immediate action must be taken by management to resolve the issues identified.

Action Priority Ratings

Risk rating	Definition
Priority 1	A high priority finding which indicates a fundamental weakness or failure in control which could lead to service or system objectives not being achieved. The Council is exposed to significant risk and management should address the recommendation urgently.
Priority 2	A medium priority finding which indicates a weakness in control that could lead to service or system objectives not being achieved. Timely management action is required to address the recommendation and mitigate the risk.
Priority 3	A low priority finding which has identified that the efficiency or effectiveness of the control environment could be improved. Management action is suggested to enhance existing controls.

Appendix C – Audit Scope

Audit Scope
We reviewed the adequacy and effectiveness of controls over the following risks: • A significant personal data breach occurs as a result of error, omission, or negligence by the Council or Council's representatives. • The Information Management Team are not aware of personal data breaches that occur, meaning that timely and appropriate action cannot be taken. • Relevant personal data breaches are not reported to the ICO or to the data subject, leading to possible financial penalties and reputational damage. Our scope included the following: • Governance, including arrangements for monitoring and oversight of personal data breaches. • Policies and procedures, including alignment to the DPA 2018 and ICO guidance and arrangements to ensure staff are aware of these. • Incident response, including reporting to the ICO and to the data subject. • Investigation of personal data breaches, including identification and dissemination of lessons learnt, and implementation of actions to prevent reoccurrence. We focused our testing on data breaches from the 2022/23 and 2023/24 financial years.