Board/Committee:	Standards and Audit Sub-Board
Date of meeting:	Thursday 11 January 2024
Title:	Data Security Breach Report
Author:	Data Protection Officer
Status:	For noting.

Purpose

To inform the Committee of any Data Security Breaches and actions agreed/taken since the last meeting

Recommendation

It is recommended that the Sub-Board note report including the breaches (by reference to Appendix A) that have arisen and the action determined by the Information Governance Group (IGG).

1.0 Background

1.1 The Information Governance Group (IGG) is formed of representatives from across the Council that meet bi-monthly.

1.2 The Group's responsibility includes:

- Establishing policy and procedures for Information Governance;
- Maintaining a log of data breaches and determining and monitoring onward action.
- Maintaining an action list and RAG register for Information Governance

1.3 The Data Protection Officer will update the IGG of any ongoing breaches and notify members of the Group of any new incidences.

2.0 Report

2.1 The appendix provides an overview of the data breaches recorded since 1st August 2022 as well as details of each individual incident. In 12 of 13 the cases, the incident was because of "human error", and 1 of "inappropriate action by staff".

None of the incidents in the reporting period reached the threshold for reporting to the Information Commissioner's Office, however due to the number of records involved, the DPO did discuss 20231101 with the ICO

and both agreed that risk to the data subjects was minimal and did not meet the threshold for reporting to the ICO.

3.0 Risk Assessment

3.1 The Information Commissioner's Office can issue fines of up to €20 million or 4% of the authority's annual turnover for serious breaches of the GDPR. Breach of the Privacy and Electronic Communications Regulations also incurs a financial penalty. The size of any monetary penalty is determined by the Commissioner, taking into account the seriousness of the breach and other factors (such as the size, financial and other resources of the data controller).

Any serious breaches put the Council at risk of the unbudgeted cost of a financial penalty, which would have to be met from the service responsible for the breach

4.0 Conclusion

The Council is required to ensure it has robust procedures in place to comply
with its obligations under the General Data Protection Regulation (GDPR). Bringing this report to the Committee's attention will assist in meeting those requirements

Financial Services comments:	None arising from this report
Legal Services comments:	
Equality and Diversity:	No comment
Climate Change implications:	
Crime and Disorder:	No comment
Service Improvement Plan implications:	
Corporate Plan:	N/A
Risk Assessment:	Within the Report
Background Papers:	None
Appendices:	Appendix A Data Breaches
Report Author/Lead Officer:	David Eland