SLOUGH BOROUGH COUNCIL

REPORT TO:	Audit and Corporate Governance Committee
DATE:	4th March 2021
CONTACT OFFICER:	Neil Wilcox; Executive Director, Corporate Operations (Section 151 Officer)
(For all Enquiries)	(01753) 875368
WARD(S):	All

PART I
FOR COMMENT & CONSIDERATION

General Data Protection Regulation Update

1. Purpose of Report

The purpose of this report is to provide Members with details on the number of breaches of General Data Protection Regulation (GDPR) / DPA2018 and any subject to legal action and to set out responsibility for GDPR / DPA2018 in the new organisational structure.

2. Recommendation(s)/Proposed Action

The Committee is requested to comment on and note details of the report.

3. The Slough Joint Wellbeing Strategy (SJWS), the Joint Strategic Needs Assessment (JSNA) and the Five Year Plan

The SJWS is the document that details the priorities agreed for Slough with partner organisations. The SJWS has been developed using a comprehensive evidence base that includes the JSNA. Both are clearly linked and must be used in conjunction when preparing your report. They have been combined in the Slough Wellbeing Board report template to enable you to provide supporting information highlighting the link between the SJWS and JSNA priorities.

3.1 **Slough Joint Wellbeing Strategy Priorities –**

The actions contained within the attached reports are designed to improve the governance of the organisation and will contribute to all of the emerging Community Strategy Priorities

Priorities:

- *Economy and Skills*
- *Health and Wellbeing*
- *Regeneration and Environment*
- *Housing*
- *Safer Communities*

3.2 **Five Year Plan Outcomes**

The actions contained within this report will assist the Council in achieving all of the five year plan outcomes

4. Other Implications

(a) Financial

There are no financial implications.

(b) Risk Management

As detailed in supporting information.

(c) Human Rights Act and Other Legal Implications

There are no Human Rights Act or other legal implications in this report

(d) *Equalities Impact Assessment, (EIA)*

There is no identified need for an EIA

5. Supporting Information

GDPR

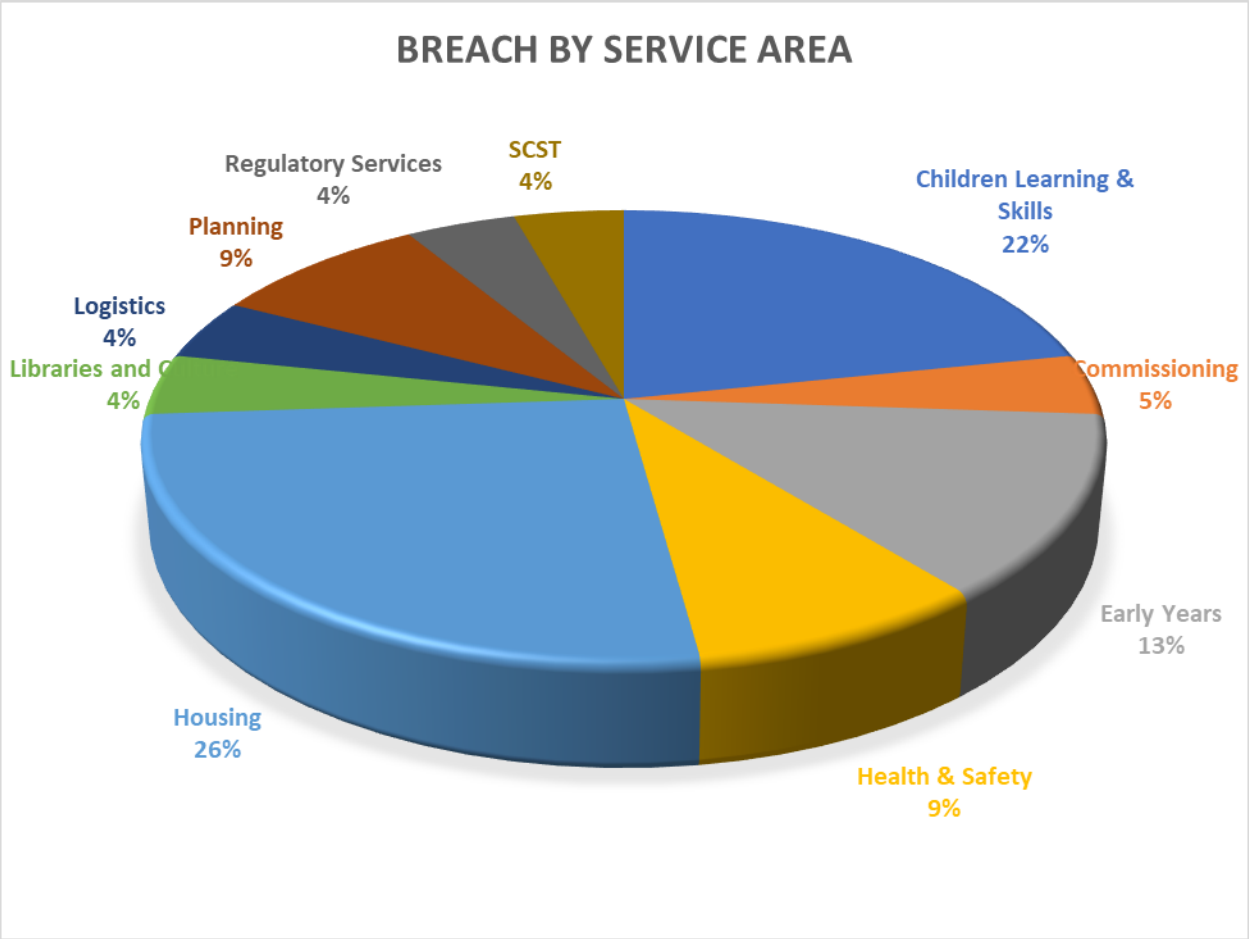
5.1 The EU's General Data Protection Regulation (GDPR) applied from 25 May 2018, when it superseded the UK Data Protection Act 1998. Significant and wide-reaching in scope, the new law elevated Council responsibilities to data protection. It expanded the rights of individuals to control how their personal information is collected and processed, and placed a range of new obligations on organisations to be more accountable for data protection.
GDPR compliance involves taking a risk-based approach to data protection, ensuring appropriate policies and procedures are in place to deal with the transparency, accountability and individuals' rights provisions, as well as building a workplace culture of data privacy and security.
UK organisations handling personal data will still need to comply with the GDPR, regardless of Brexit.
A breach could cause significant impact on SBC finances.
GDPR applies to all – this means that any company that works with information relating to EU citizens will have to comply with the requirements of the GDPR.
GDPR introduces a common data breach notification requirement – Data controllers must notify the Data Protection Authorities as quickly as possible, where applicable within 72 hours, of the data breach discovery.

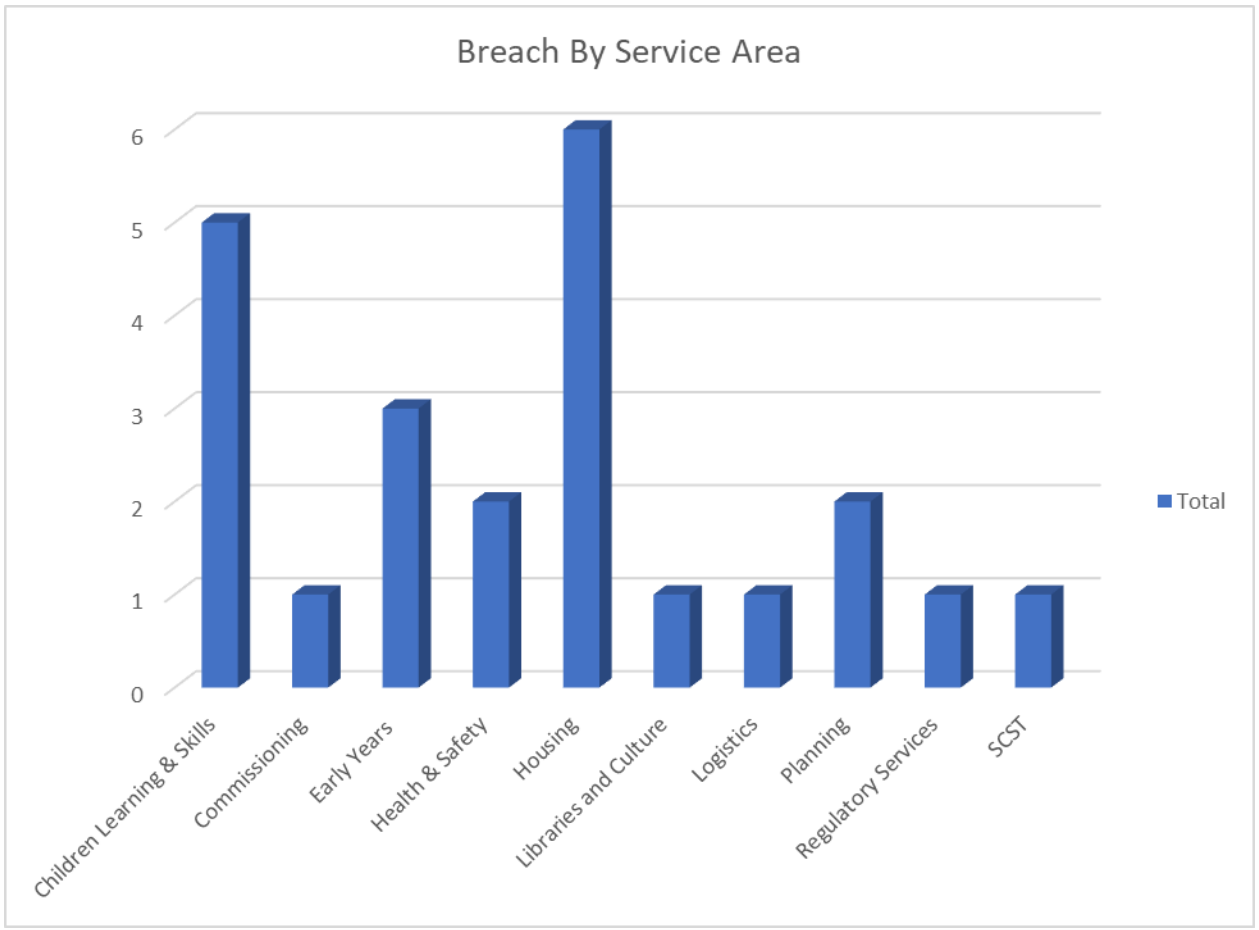
5.2 Monitoring of incidents / breaches is performed by the Information Governance team, instances are assessed, recorded and reported to the Information Commissioners Office if required where a significant breach.

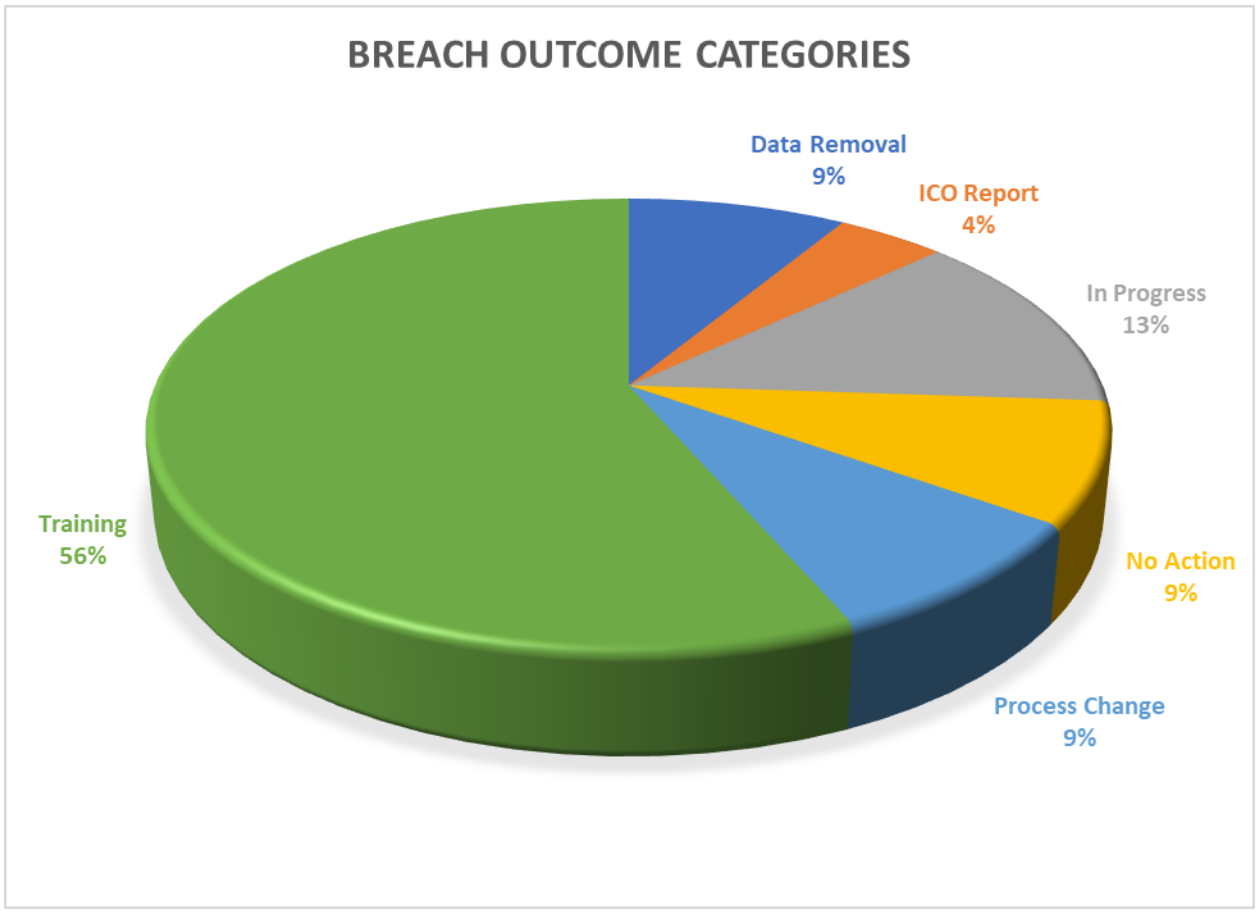
For the financial year 1/4/20 to date, there were a total of 23 incidents recorded, of these 1 was reported to the ICO, in this instance the ICO deemed no further action necessary and there was no fine applied to SBC.

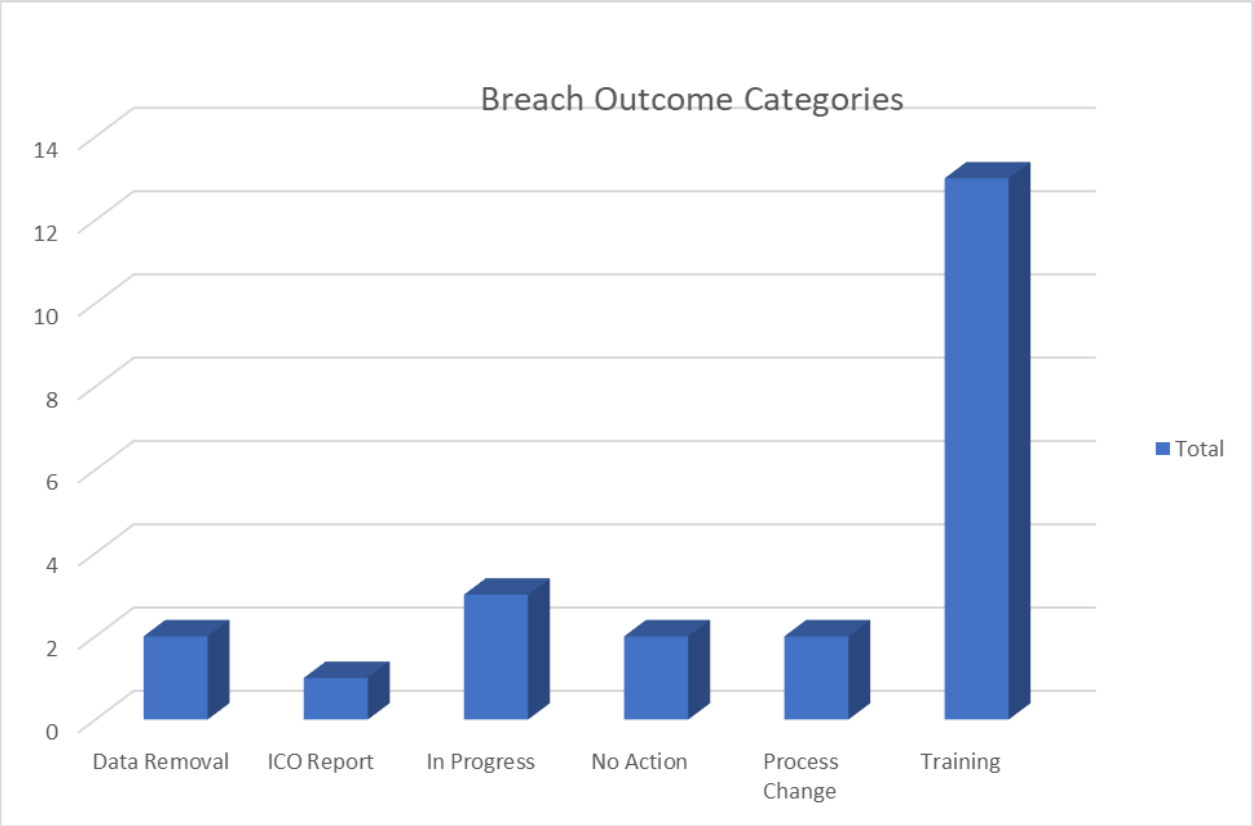
There were 1 technical breaches / system compromised of a hosted system and the remaining 22 incidents were data disclosed in error by staff action. All these incidents were reviewed, controlled and mitigated to avoid the need of any further action.

The breaches occurred across multiple council departments. The risk of re-occurrence was removed in most instances by enhanced training and in two of the instances a change in process was implemented to improve compliance.




Breach By Service Area
6
5
4
3
2
1
0
Children Learning & Skills
Commissioning
Early Years
Health & Safety
Housing
Libraries and Culture
Logistics
Planning
Regulatory Services
SCST
Total


BREACH OUTCOME CATEGORIES
Data Removal
9%
ICO Report
4%
In Progress
13%
No Action
9%
Process Change
9%
Training
56%



5.3 Ongoing monitoring - The Councils information governance board receives monthly reports and reviews lessons learnt. Any significant breaches are also reported to CMT by the Councils Senior Information Risk Officer (SIRO).

5.4 DPO Role - Since May 2018 the councils DPO role has been covered internally with an Interim appointment, the recruitment has been delayed previously but more recently due to the council's wider reorganisation.

The UK GDPR introduced a duty to appoint a data protection officer (DPO) if you are a public authority or body, or if you carry out certain types of processing activities.
This role assists in the monitoring of internal compliance and to inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner's Office (ICO).
The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level, a DPO can be an existing employee or externally appointed and can help you demonstrate compliance and are part of the enhanced focus on accountability.

The DPO's tasks are defined in Article 39 as:

- to inform and advise about our obligations to comply with the UK GDPR and other data protection laws;
- to monitor compliance with the UK GDPR and other data protection laws, and with our data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor, data protection impact assessments;
- to cooperate with the ICO; and

- to be the first point of contact for the ICO and for individuals whose data is processed (employees, customers etc).

The DPO's tasks cover all personal data processing activities, not just those that require their appointment under Article 37(1).

- When carrying out their tasks the DPO is required to take into account the risk associated with the processing that is being undertaken. They must have regard to the nature, scope, context and purposes of the processing.
- The DPO should prioritise and focus on the more risky activities, for example where special category data is being processed, or where the potential impact on individuals could be damaging. Therefore, DPOs should provide risk-based advice to the organisation.
- Decision not to follow the advice given by the DPO, should be documented with reasons to help demonstrate accountability.

5.5 The DPO role has been identified in the initial proposed structure for IT with a direct line of reporting to the lead on Information Governance, although as the structure has been withdrawn a decision on revised structure is pending further consultation.

6. Comments of Other Committees

There are no comments from other Committees

7. Conclusion

Members are requested to consider and note details of the report.

8. Appendices Attached

N/A

9. Background Papers

None