Portsmouth CITY COUNCIL

THIS ITEM IS FOR INFORMATION ONLY
(Please note that "Information Only" reports do not require Integrated Impact Assessments, Legal or Finance Comments as no decision is being taken)

Title of meeting:	Governance & Audit & Standards Committee
Subject:	Data Security Breaches Report
Date of meeting:	29 September 2022
Report by:	Elizabeth Goodwin, Senior Information Risk Owner
Wards affected:	All

---

1. Requested by

Governance & Audit & Standards Committee

2. Purpose

To inform the Committee of any Data Security Breaches and enable them to determine whether any trends appear and whether any further actions should be recommended.

3. Information Requested

The appendix provides an overview of the breaches that have occurred since March 2022

70% of all incidents were as a result of human error. In each case, if the member of staff concerned had not completed the mandatory Data Protection e-learning within the last 12 months, they were required to do so.

There was an increase in this reporting period of breaches caused by inappropriate action taken by staff (i.e. not complying with council policies and/or procedures). The Information Governance team has worked with the respective areas of the council to ensure staff are aware of the correct procedures so that similar errors are not repeated.

It is planned that a regular series of messages goes out to all staff (using the "In The Know" communication, to raise awareness of data breaches and how they can be avoided.

Two of the incidents in the reporting period reached the threshold for reporting to the Information Commissioner's Office (ICO). In both cases, the incident involved records

Portsmouth CITY COUNCIL

THIS ITEM IS FOR INFORMATION ONLY
(Please note that "Information Only" reports do not require Integrated Impact Assessments, Legal or Finance Comments as no decision is being taken)

being accessed by individuals without a business need to. The first of these incidents involved a member of staff employed by the council and the formal action policy was instigated. The ICO confirmed it was satisfied with our investigation, that all necessary actions had been taken and considered the case closed.

The second of these breaches related to a member of staff employed by one of the council's contractors and the outcome from the ICO is still awaited.

The council takes these matters very seriously and a number of measures are in place to deter staff from inappropriately accessing records, for example:-

- Access to the case recording system used by Children's Social Care (Mosaic) is regularly audited to identify anomalies in access to records and any concerns are followed up by the relevant manager.
- Highly detailed reports can be run to show who accessed the system and what information was viewed.
- All staff in social care sign a declaration before being granted access to the system, stating they will not access records unless they have a business need to. A reminder of this will be sent.

The highest number of breaches continue to be caused by emails being sent to the wrong recipient. This is consistent with national trends as reported by the Information Commissioner's Office. The council is currently working on the next phase of the rollout of Microsoft 365 which will include Data Loss Prevention Tools. A set of bespoke rules will be created to examine email messages and files for pre-defined sensitive information and either display a warning to the user to check the information and recipient or actively block the email or file sharing from taking place. The council is confident this will significantly reduce the number of errors.

Following a request from the Governance & Audit & Standards Committee, some additional information is included in this report relating specifically to data breaches in Children's Social Care as it was noted the number of incidents in this area is typically higher than others.

This is thought to be due to a number of factors:-

- The culture encouraged by the Director of Children's Services & Education, the Caldicott Guardian and Senior Management Team whereby officers feel they can proactively report incidents
- The large volume of personal data being processed
- The frequency with which communications are sent outside the council

Portsmouth CITY COUNCIL

THIS ITEM IS FOR INFORMATION ONLY

(Please note that "Information Only" reports do not require Integrated Impact Assessments, Legal or Finance Comments as no decision is being taken)

All breaches are robustly investigated by a senior manager and overseen by the Caldicott Guardian with involvement from the Director when necessary. This has proved to be to the satisfaction of the Information Commissioner's Office when cases have been reported.

Monthly meetings are held between the Caldicott Guardian and the Information Governance Team to identify areas of concern and provide advice, guidance and training to staff to minimise the risk of breaches re-occurring. Procedures are always reviewed to see if changes can be made to reduce the need to process personal data and therefore the risk of disclosing it in error.

The Information Governance Team will continue to work with all areas of the council to reduce the number of breaches and report to this committee.

……
Signed by (Director)

Appendices:

One Appendix - Appendix A

Background list of documents: Section 100D of the Local Government Act 1972

The following documents disclose facts or matters, which have been relied upon to a material extent by the author in preparing this report:

Title of document	Location
None	