East Herts Council Report

Audit and Governance Committee

Date of meeting: Wednesday 28 May 2025

Report by: Tyron Suddes – Information Governance and Data Protection Manager

Report title: Data Protection Update

Ward(s) affected: (All Wards);

Summary – To provide an update on the council's response to reported data breaches and subject access requests

RECOMMENDATIONS FOR Audit and Governance Committee

a) That the Committee notes the content of the report and provides any observations to the Information Governance and Data Protection Manager.

1.0 Proposal(s)

1.1. As above

2.0 Background

2.1. This report provides a regular update on the council's response to reported data breaches and subject access requests.

2.2. There have been eleven reported breaches from 1st October 2024 to 1st April 2025, none were deemed serious enough to require onward reporting to the Information Commissioner's Office (ICO).

2.3. Of the reported breaches:

2.3.1. Nine were due to correspondence being sent to an incorrect recipient;

2.3.2. One was due to additional information being moved over during the BEAM data transfer and;

2.3.3. One was due to details being incorrectly published on the council's planning portal.

2.4. The following actions were taken to prevent similar breaches from occurring in future:

2.4.1. Apologies and Notifications:

2.4.1.1. Apologies were issued to affected data subjects.

2.4.1.2. Data subjects were informed of errors where necessary.

2.4.2. Recipient Actions:

2.4.2.1. Incorrect recipients were contacted and asked to delete or destroy data.

2.4.2.2. Confirmation was received that data was deleted or not accessed in most cases.

2.4.3. Staff Reminders and Training:

2.4.3.1. Staff responsible for breaches were advised to retake the data protection e-learning course.

2.4.3.2. Reminders were issued to staff to handle personal data carefully, verify details before approving changes, and clear their auto-complete cache to avoid similar errors.

2.4.4. Planning Portal Updates:

2.4.4.1 Immediate removal of incorrectly published data.

2.4.4.2. Updates were made to prevent future publication of personal details in a way that could lead to a data breach.

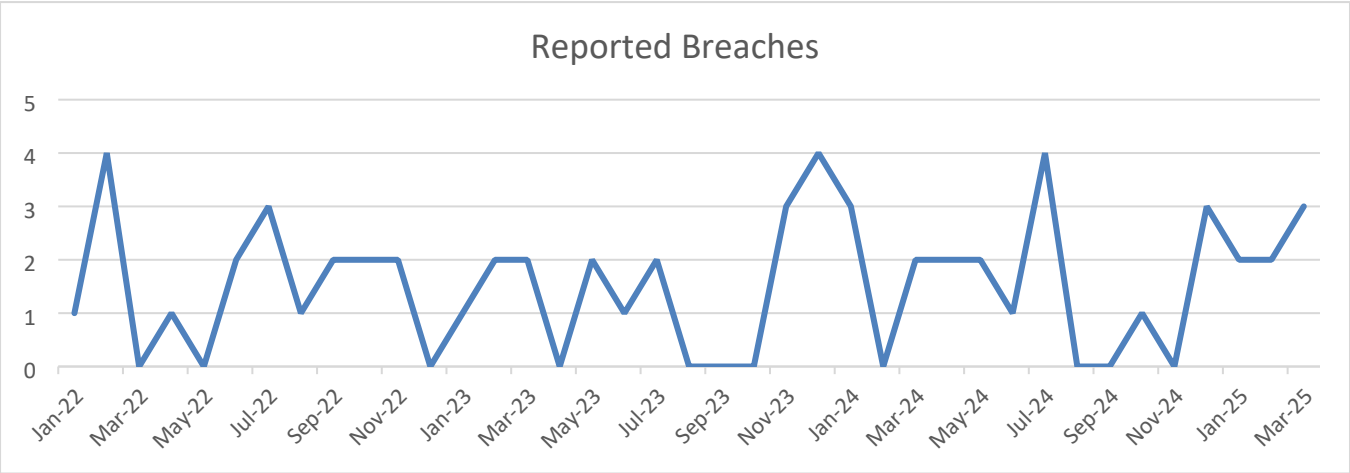
2.4.5. Other Preventative Measures:

2.4.5.1 Processes for council tax accounts were updated to ensure contact details are verified and errors avoided.

2.4.5.2. Assurance was sought from software providers on rectifying issues.

2.4.5.3. Email recall attempts were made when applicable.

2.5. The number of data breaches over the last reporting period remains acceptable, particularly given the amount of personal data the council processes. Additionally, this indicates that staff can recognise and know how to report suspected data breaches and have done so within the time limit set out in the council's Data Breach Policy. The table below gives an overview of reported data breach trends:



2.6. The council's data breach incidents and responses were audited in October 2024 and we received substantial assurance with two low priority recommendations that have now been actioned through the Data Breach Policy.

2.7. There have been eleven subject access requests from 1st October 2024 to 1st April 2025. All requests were processed and responded to within the statutory time limit.

3.0 Reason(s)

3.1. At its meeting on 17th November 2020, the Audit and Governance Committee requested that it receives reports on data protection matters.

3.2 At paragraph 8.1.8(n) of the Constitution, the Audit and Governance Committee has a role in considering the council's Data Protection policies and procedures.

4.0 Options

4.1. The Committee requested an update and so there are no alternative options to consider.

5.0 Risks

5.1. Data Breaches can pose a financial and reputational risk to the council if they are not reported and dealt with correctly, however, the council, through e-learning, virtual classroom training, shared learning and updated policies and procedures has raised awareness around data breaches and how to prevent and report these where required. Additionally, through regular reporting of breaches, the council can identify trends and possible actions to prevent these reoccurring.

5.2. Similarly, subject access requests, if not responded to correctly and within the statutory one-month time frame, can pose financial and reputational risks to the council. This report provides reassurance the council continues to respond to these requests in line with legislation.

6.0 Implications/Consultations

Community Safety

No

Data Protection

Yes - regular updates on data protection aim to provide assurance that the council remains compliant with data protection legislation. Equally, updating on data breaches and subject access requests provides assurance that the council remains compliant in these areas.

Equalities

No

Environmental Sustainability

No

Financial

Yes - A serious data breach could result in the council facing substantial financial penalties, emphasising the importance of monitoring performance and responses to those breaches that arise from time to time.

Health and Safety

No

Human Resources

No

Human Rights

No

Legal

No – other than as identified above.

Specific Wards

No

7.0 Background papers, appendices and other relevant material

7.1. None

Contact Member

Executive Member for Corporate Services

Joseph.Dumont@eastherts.gov.uk

Contact Officer

Tyron Suddes, Information Governance and Data Protection Manager

Tyron.Suddes@eastherts.gov.uk

Report Author

Tyron Suddes, Information Governance and Data Protection Manager

tyron.suddes@eastherts.gov.uk