

East Herts Council Report

Audit and Governance Committee

Date of meeting: Tuesday 24 January 2023

Report by: Councillor George Cutting – Executive Member for Corporate Services

Report title: Data Protection Update

Ward(s) affected: (All Wards);

Summary – To provide an update on data protection compliance, including data breaches and subject access requests (SARs)

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 six-monthly update on data protection compliance, including the number of data breaches reported and responded to, and the number of SARs received in the six month reporting period.

2.2 Since the last update given on the 31 May 2022, the actions for the GDPR Roadmap 2021/22 are now complete and the council's compliance will be monitored under the final 'Govern' strand to ensure that changing legislation is managed, and overall compliance is regularly audited.

2.3 The successful implementation of the roadmap is supported by the recent Information Governance 2022-23 Audit in which the council was given

substantial assurance in information management and reporting as required by the UK GDPR.

2.4 As part of a regular data protection update, the committee requested an update on data breaches and SARs.

2.5 There have been a total of eleven reported data breaches from the beginning of May 2022 to the end of October 2022, one of which was reported to the Information Commissioner's Office (ICO) as, although it was unlikely the risks of the breach would be realised, the breached data included sensitive data.

2.6 The following actions were taken in response to the reported breach:

2.6.1 The published data was immediately removed.

2.6.2 The software used to publish the information has had an additional function enabled which will prevent this type of data from being published on the council's website.

2.6.3 An audit has been carried out to ensure there is no similar published information elsewhere on the council's website.

2.7 The ICO was satisfied with the actions taken and measures put into place to rectify the breach and prevent similar breaches from occurring in the future and so took no further action.

2.8 The other ten breaches were caused by human error whereby:

2.8.1 There were three instances where an email was sent to an incorrect recipient.

2.8.2 There were four instances where a letter was sent in error to an incorrect recipient.

2.8.3 There were two instances where staff member's folders were made available to another staff member following migration to MS365.

2.8.4 Incorrect details were entered into the direct debit system.

2.9 Where breaches were due to human error, the following action(s) were taken:

2.9.1 Messages were recalled where possible and unauthorised recipients were asked to delete data as soon as possible and confirm once done. An explanation and apology were sent to affected data subjects where appropriate.

2.9.2 Where migration issues resulted in a breach, IT will now ensure that the service desk do not make changes to user profiles in the lead up to the relevant service migration. If urgent changes are required, these will only be made by senior managers.

2.9.3 Incorrect details were immediately corrected.

2.9.4 Staff members responsible were reminded of the serious consequences of a data breach, and where appropriate, were given data breach training by the Information Governance and Data Protection Manager.

2.9.5 The data protection best practice page has been updated to reflect lessons learnt and this was communicated to all staff.

2.10 The amount of breaches over the last six month period remains low, although has increased since the last reporting period which may reflect that staff are more aware of what constitutes a data breach and how to report these.

2.11 Short term actions have been put in place and monitored and wider actions, particularly related to human error breaches, are currently being considered following the council's migration to MS365 and the additional preventative tools which may be implemented.

2.12 There have been a total of eight SARs received from the beginning of May 2022 to the end of October 2022. All requests were responded to within the statutory time limit.

3.0 Reason(s)

3.1 At its meeting on 17th November 2020¹, the Audit & Governance Committee requested that it receive regular reports, at six monthly intervals, on GDPR and data protection matters.

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 and virtual classroom training and updated policies and procedures has limited the amount of breaches. 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 that the council continues to respond to these requests in line with legislation.

6.0 Implications/Consultations

6.1 None

Community Safety

No

¹ [Minute 248](#)

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

No

Health and Safety

No

Human Resources

No

Human Rights

No

Legal

None, 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

George.Cutting@eastherts.gov.uk

Contact Officer

Head of Legal and Democratic Services,

Contact Tel. No. 01279 502170

James.Ellis@eastherts.gov.uk

Report Author

Tyron Suddes, Information Governance and
Data Protection Manager

tyron.suddes@eastherts.gov.uk