East Herts Council Report

Executive

Date of meeting: 6 July 2021

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

Report title: East Herts Council Data Breach Policy and procedures

Ward(s) affected: All

Summary – This report presents the revised East Herts Council Data Breach Policy (Appendix A) and its related revised procedural documents, the Data Breach Flowchart (Appendix B), the Staff Data Breach Report Form (Appendix C) and the Data Breach Report template (Appendix D).

The policy updates and replaces the Data Security Breach Management Policy.

In a report taken to Overview and Scrutiny Committee on 8 June 2021, the committee supported the proposal to recommend this policy and procedures to Executive for adoption.

Executive is asked to consider the revised policy and procedures, propose any amendments and **adopt** the policy and procedures following any amendments.

RECOMMENDATIONS FOR Executive

(a) That the revised Data Breach Policy and its related procedural documents are adopted following any amendments.

(b) That the Information Governance and Data Protection Manager be authorised to make any minor amendments that may be required, in consultation with the Head of Legal and Democratic Services.

1.0 Proposal(s)

It is proposed that Executive considers the revised Data Breach Policy and its related procedural documents and adopt it having first proposed any amendments it sees fit.

2.0 Background

2.1 Following an audit of the council's information management arrangements, it was identified that although the council had documented its data breach procedures, its Data Breach Policy had not been formally adopted.

2.2 The audit recommended that the policy should be adopted and then communicated to all staff.

2.3 The draft policy and procedures went before Overview & Scrutiny Committee on 8 June 2021 and was recommended to Executive for adoption without any further amendments.

3.0 Reason(s)

3.1 The revised policy and procedures ensure that the council has robust and updated breach detection, investigation and internal reporting procedures in place that facilitate decision-making about whether or not to notify the Information Commissioner's Office ("the ICO") or the affected individuals, or both. It also ensures that record is kept of any personal data breaches, regardless of whether notification is required or not so that council is able to demonstrate compliance with the UK GDPR.

3.2 The policy initially sets out what data breaches are and how to recognise them. Initial steps to be taken upon notification of a suspected breach are then laid out, including containing the breach itself, determining the full particulars of it, working out what needs to be done to resolve and remedy the situation properly and establishing who needs to be notified internally. Officers that need to be notified are determined following a risk assessment of the potential breach. This initial process is recorded in the Staff Data Breach Report Form.

3.3 The policy then sets out the steps for a full investigation and assessment of the potential breach by determining who will be affected by the breach and to what degree, how much data is involved, how many data subjects will be affected, the consequences of the breach and more. Additionally, some personal data breaches must be notified to the ICO and to the individual data subjects whose data is involved in the breach. This policy sets out

some key considerations to help determine who needs to be notified. The process above is recorded in the Data Breach Report template.

3.4 The policy and its related procedures have been drafted to ensure that suspected breaches are contained quickly and reported, if required, within the 72 hour timeframe set out by the Information Commissioner's Office.

3.5 The policy and data breach report template ensure that, once the breach itself is resolved and all necessary parties have been notified, steps are taken to prevent similar breaches from occurring in future. It sets out that all data breaches, regardless of risk, are recorded in a data breach log and reported half yearly to Leadership Team and Audit and Governance Committee so that existing practices, procedures, and measures can be evaluated, and changes and improvements implemented if required.

3.6 The updated data breach procedure flowchart reflects the contents of the policy in a summary chart of what needs to be done if a breach is suspected.

4.0 Options

4.1 Not to adopt this policy and maintain the existing data breach procedures and guidance without an adopted policy document. **NOT RECOMMENDED** as this would work against the audit recommendations and the council's aim to ensure consistently robust data breach reporting procedures and compliance with the UK GDPR.

4.2 To consider and adopt this policy and procedures. **RECOMMENDED** as a means of ensuring that the council has an up-to-date policy document in place to ensure that data breach best practice is adopted and applied.

5.0 Risks

5.1 Failing to notify the Information Commissioner's Office and/or data subjects of a breach when required to do so can result in significant fines which would have a high impact on the council.

5.2 There may be additional reputational implications if the Information Commissioner's Office were to investigate the council following a failure to notify regardless of the final decision.

6.0 Implications/Consultations

Community Safety

No

Data Protection

Yes – The adoption of this policy would ensure that the council has a robust breach reporting process in place to ensure that it is able to detect, and notify relevant parties of breaches, on time and provide and/or record the necessary details where required.

Equalities

Yes – The policy aims to ensure that equality best practice is applied to the council's data breach reporting procedures and guidance.

Environmental Sustainability

No

Financial

No

Health and Safety

No

Human Resources

No

Human Rights

No

Legal

Yes – The Council is under an obligation to ensure it complies with UK data protection law, and the adoption of this policy strengthens the council's compliance with the relevant data protection legislation.

Specific Wards

No

7.0 Background papers, appendices and other relevant material

7.1 Appendix A – DRAFT – East Herts Council Data Breach Policy 2021

7.2 Appendix B – Data Breach Procedure Flowchart – 2021

7.3 Appendix C – Staff Data Breach Report Form – 2021

7.4 Appendix D – Data Breach Report Template - 2021

Contact Member

Cllr George Cutting
Executive Member for Corporate Services
01279 651361
george.cutting@eastherts.gov.uk

Contact Officer

James Ellis
Head of Legal and Democratic Services

01279 502170

James.Ellis@eastherts.gov.uk

Report Author

Tyron Suddes
Information Governance and Data Protection Manager
01279 502148
Tyron.Suddes@eastherts.gov.uk