WELWYN HATFIELD

Version **5.0**

Data Breach Procedure

Scope:	This procedure applies to all employees, councillors, and processors. This procedure impacts residents and service users of the council.
Effective Date:	13th April 2026
Review Date:	13th April 2028
Author:	Kyle Houston, Governance Policy Officer
Policy Owned by:	Gavin Ramtohal, Assistant Director (Legal and Governance)
Statute:	UK General Data Protection Regulations Data Protection Act 2018 Data Use (and Access) Act 2025
National Standards and Guidance	Data Breach ICO Guidance Personal Data ICO Guidance European Commission Guidelines on Personal Data Breach
Related Policies	Data Protection Policy Acceptable Use of IT Policy Information Governance Appeal Procedure

1 Introduction

1.1 The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA) outline the requirements for an organisation to lawfully process personal information and what to do in the event of a data breach.

1.2 A data breach is where personal information is processed unlawfully. This may include disclosure to third parties, unplanned destruction or alteration of information, or unauthorised access to personal information.

1.3 The Data Breach Procedure should be read in conjunction with the Data Protection Policy, which contains data protection definitions, explains the Council's obligations under the legislation, how processing should be conducted appropriately, and the measures in place to reduce the risk of a data breach.

1.4 The Council could incur financial penalties where a data breach occurs and it is not appropriately handled. The GDPR and DPA set a maximum fine of £8.7 million or 2% of annual global turnover, whichever is greater, for data breaches. The ICO may use other corrective powers contained in Article 58 of the GDPR.

1.5 This procedure sets out the actions that must be taken in the event of a suspected data breach, and how it will be assessed and handled.

1.6 This procedure applies to staff, and third parties where they are acting as a processor and it is specified in their contract. For further information on whether a third party is a processor, please review the Data Protection Policy and/or contact dataprotection@welhat.gov.uk.

2 Data Breach Procedure

2.1 If a suspected data breach is identified, staff must immediately inform the governance team via dataprotection@welhat.gov.uk immediately. The details of the breach, any evidence of the breach, any actions taken, and the potential harm should be communicated.

2.2 The governance team will assess whether the suspected data breach is a legitimate data breach.

2.3 The governance team will undertake a Data Breach Risk Assessment (contained in Appendix B) to determine the severity of the incident and the risk of harm to the impacted subject(s). Where necessary, the governance team will use the Information Commissioner's Office (ICO) self-assessment tool if the outcome of the Data Breach Risk Assessment is not conclusive.

2.4 The Council has 72 hours to assess the risk of the data breach and whether the risk of harm is substantial to the impacted subject(s). This deadline will begin once the suspected data breach is identified by any member of staff. If a suspected breach is not raised immediately this may impact the Council's ability to assess the risk and handle the data breach.

2.5 If the Council determines that the risk of harm to data subject(s) is high and/or the data breach is substantial, they will inform the ICO within the 72 hours deadline. If a full assessment has not been conducted within 72 hours and there is not a firm understanding of the risk involved, they will inform the ICO and provide further information as it is discovered.

2.6 Where notification to the ICO is not made within 72 hours and the Council decides to notify the ICO outside of the deadline, it shall be accompanied by an explanation of why the breach was initially considered to be low risk and not substantial or the reasons for delay.

2.7 The governance team will inform the ICO via their online data breach report form.

2.8 If the Council determine there is a high risk to the impacted subject(s), they will be notified of the breach. Specifically, they will be notified that a breach has occurred, the nature of the breach, confirmation that they are impacted, an explanation of how they are impacted, the assessed and potential risk, the measures taken, where possible any guidance on how they may reduce the assessed risk, and a copy of the Information Governance Appeal Procedure.

2.9 The following are the only instances where notification will not be given:

a. The Council is unable to contact the subject, and it would involve disproportionate effort to contact the subject.
b. The Council has taken the necessary actions to mitigate the assessed risk.
c. The Council has determined that discussion with the impacted subject(s) would cause disproportionate stress and impact their health.

Where a valid Data Protection exemption removes the right to be informed of a data breach.

2.10 The Information Governance Appeal Procedure will contain details on how an impacted subject may appeal the Council's handling and/or the outcome of the data breach assessment.

3 Data Breach Register and records

3.1 Under Article 33(5) of the UK GDPR, the Council is required to maintain a data breach register.

3.2 This Register includes the date the breach occurred, was identified, and raised to Governance; the date the assessment was concluded; a brief description of the breach's nature (excluding personal details), the responsible service area or processor, whether it was a data breach or not, the assessed risk level, the measures taken, whether the impacted subject(s) was informed and the justification for whether the impacted subject(s) was informed or not, whether the ICO was notified of the breach and the actions that the ICO recommended, and whether an appeal was received and its outcomes.

3.3 The Data Breach Register will be maintained indefinitely. A review will be conducted annually to ensure no personal information identifying the impacted subject(s) is recorded in the register, and if any personal information is contained, it will be deleted.

3.4 Data Breach Risk Assessment Forms will be kept for 6 years after their creation. These forms will be deleted annually according to year, and not based on the exact date of the form's creation

4 Monitoring

4.1 The Governance team are responsible for reviewing the Data Breach Procedure and providing data protection services in line with the Data Protection Officer's guidance and instructions.

4.2 Updated versions of this procedure will be reviewed and agreed with the Senior Leadership Team. This procedure may be reviewed and agreed in advance if a weakness is found, there are legislative changes, or if the Information Commissioner's Office makes any recommendations.

5 Version History

Version no.	5.0	**Date effective:**	13th April 2026
Full / partial review?		Full	
Brief summary of changes:		The Data Breach Procedure was rewritten to expand on the obligations of the Council, new guidance was referenced, an expansion on the section 3 was included, and a monitoring section was included.	
Staff consultation (teams):		SLT	
Author:		Kyle Houston, Governance Policy Officer	

Appendix A – Roles and Responsibilities

Stakeholder	Responsibilities
Chief Executive Officer	Accountable for the effectiveness of the council's arrangements for complying with the Data Protection Act 2018 and UK General Data Protection Regulations.
Executive Director (Finance & Transformation) **Section 151 Officer**	To ensure that the council has an adequately resourced and effective Governance Team and Data Protection resources.
Assistant Director (Legal & Governance) **Monitoring Officer**	Responsible for ensuring the Governance team is operating effectively and complying with their responsibilities.
Governance Services Manager **Data Protection Officer**	Responsible for managing the Governance Team and ensuring that Governance Officers fulfil their designated responsibilities. Accountable for the Council's Data Protection services and responsible for monitoring compliance with the Data Protection Act 2018 and UK General Data Protection Regulations. Responsible for approving procedures where outlined in procedures and documents.
Governance Policy Officer	Responsible for reviewing and drafting data protection policies, processing data protection services, and acting on the instruction of the Data Protection Officer.
Directors and Managers acting as Project leads	Responsible for ensuring that processing activity is compliant with the data protection policy and other associated policies/procedures.
Staff	Responsible for upholding the principles and standards outlined in the data protection policy and other associated policies/procedures.
Processors	Responsible for complying with their contract and/or Data Sharing Agreement.

Appendix B – Data Breach Assessment Form Template

Data Breach Assessment Form

Last review date	
Service Area responsible for breach	
Service area contact	
Governance contact	
Summary of breach Include how the breach was identified, how the breach occurred, and any influencing details about the impacted subject, such as health conditions or vulnerabilities (Do not identify them).	

Details of the breach

Date breach occurred	
Date breach was identified	
Date breach was raised to governance	
Breach type	☐Disclosure to third party ☐Unplanned deletion/alteration ☐Unauthorised access
What caused the breach?	☐Human error ☐Technical error
Personal information affected or disclosed	
Special category personal information affected or disclosed	
(if disclosed) Details an individual may be able to infer from information	
Officer(s) responsible	
System/software involved	
Details of how breach occurred	

Impact of the breach

Number of subjects affected	
Are the subjects vulnerable individuals? (children, disabled individuals, etc…)	
How might the breach affect the impacted subject(s)	
(If disclosed) Does the impact subject(s) have any association to the third party?	

Actions following the breach

Will the impacted subject(s) be made aware of the breach?	
Please justify the decision to inform or not inform impacted subject(s)	
Has this case been escalated to the ICO? If yes, please include the ICO's reference number and the outcomes.	
Actions recommended	