Procedure for Reporting Data Protection Breaches

Version Control:

Version	Amended by	Date	Summary of Changes
1.0		May 2018	
2.0	HIAG	January 2023	

Contents

1. Introduction

1.1. This procedure applies to all staff and volunteers working for the Council and it applies to any actual or suspected loss of personal data, and to any "near miss" in which a personal data breach was narrowly avoided.

1.2. This procedure should be used to report all breaches of confidentiality, loss of data, unauthorised disclosure and information security breaches, whether actual or suspected. This covers information held and shared in different formats (paper, electronic or verbal).

1.3. A **personal data breach** is defined by the Information Commissioner's Office (ICO) as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data." A report must be made to the ICO within 72 hours of the breach occurring, if the Council's Data Protection Officer (DPO) determines that there is a risk to the rights and freedoms of the individuals affected.

1.4. Due to the mandatory time period of 72 hours, you must report any actual or suspected personal data breaches to the Council's Data Protection Officer immediately through the formal reporting mechanism on the Council's intranet and by informing your Manager.

1.5. The Council must report certain types of breaches to the ICO, and large fines may be payable for a personal data breach. All staff and volunteers have a responsibility to report a suspected or actual personal data breach. Failure to do so may be considered a breach of the Council's Data Protection Policy and may result in disciplinary action.

1.6. When a personal data breach occurs or is suspected to have occurred, the ICO requires organisations to consider whether the breach poses a risk to people. Organisations must consider the likelihood and severity of the risk to people's rights and freedoms, following the breach. Where a breach is sufficiently serious, the assessment and report to the ICO must happen within 72 hours of the breach by the Council's DPO.

1.7. Where there is a risk that Credit or Debit Card information may have been compromised, the Card Data Security Incident Response Plan should also be followed.

1.8. There is a separate, related procedure to report and investigate all **information security incidents** whether actual or suspected. This is located on the ICT Intranet under ICT Standards and Policies and can be found at this link: Information Security Incident Reporting Procedure .pdf

1.9. Information security incidents may involve the loss of personal data and include loss or theft of devices (phone, laptop, tablet etc.), unauthorised attempts to access systems or data, hacking, password attacks or account compromise, malware incidents, phishing incidents and Denial of Service (DoS) attacks.

2. Procedure

2.1. If you suspect a personal data breach has occurred, you must report it ***immediately*** to the Council's Data Protection Officer (the DPO) as the Council is under a duty to report serious incidents within 72 hours of becoming aware of them.

2.2. Breaches should be reported to the DPO Glen Egan immediately through the formal reporting mechanism on the Council's intranet and by informing your Manager. The DPO's

email address is gegan2@hillingdon.gov.uk.

2.3. The DPO will conduct an initial investigation and risk assessment, using the ICO template, to ascertain the nature and seriousness of the incident. The ICO time limit means that it is imperative that this assessment is done without delay.

2.4. If a breach meets the threshold requiring a report to the ICO, the DPO will inform the Chief Executive of this fact and shall also inform the ICO as soon as possible and no later than 72 hours from the time the Council became aware of the breach. This is further explained in section 5 of this Procedure.

2.5. The DPO does not need to have full details of the personal data breach available prior to making a notification to the ICO. If the DPO believes, on initial assessment, that there is a likelihood that the breach will meet the notification requirements, then the DPO will make the initial notification within 72 hours and update the ICO as and when further information becomes available.

2.6. The DPO will maintain a record of incidents, including a risk assessment, the outcomes and resulting recommendations made.

2.7. The DPO will report breaches to the Chief Executive, recommendations reported twice yearly to the CMT, and will implement any recommendations through the Hillingdon Information Assurance Group (HIAG).

3. Breach Management Team

3.1. The Council's DPO will, if they consider it necessary to do so, chair a breach management team to assist in responding to a breach. The exact makeup of this team will depend on the nature and the seriousness of the breach and what skills and resources are required to respond.

3.2. The core team will be drawn from HIAG and comprise of representatives from ICT, Legal Services, Risk & Audit, Human Resources and the Communications Team as well as representatives from the affected service areas. The composition of the team will depend on the exact nature of the breach.

4. Guidance

4.1. What ***is a personal data breach?*** Breaches can be categorised according to the following three information security principles:

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.
- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.

A breach may involve a combination of these elements.

4.2. ***Assessing Risk & High Risk*** Although UK GDPR introduced the obligation to notify a

breach to the ICO and/or to those affected, there is not a requirement to do so in all circumstances:

- Notification to the ICO is only triggered where a breach is likely to result in a risk to the rights and freedoms of individuals.
- Communication of a breach to the individual is only triggered where it is likely to result in a high risk to their rights and freedoms.

4.3. A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. This includes loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include other significant economic or social disadvantage to those individuals.

4.4. A breach will be considered to pose a high risk to the rights and freedoms of individuals where the breach may lead to physical, material, or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation.

4.5. When the breach involves *special category personal data* that reveals racial or ethnic origin, political opinions, religious beliefs or philosophical beliefs, or trade union membership, or includes genetic data and biometric data for the purpose of identifying a natural person, data concerning health or data concerning sex life or sexual orientation, or criminal convictions and offences or related security measures, it should be assumed that there will be a high risk to the rights and freedoms of individuals.

4.6. Factors to consider:

- Nature of the breach
- Nature, sensitivity, and volume of the data
- Ease of identification
- Severity of consequences for data subject(s) - for instance identity theft or fraud, physical harm, psychological distress, humiliation, or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm
- If there has been a loss of confidentiality is the 3rd party "trusted" - the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the ICO, or to the affected individuals.
- Special characteristics of the individual (children, vulnerable adults etc)
- The number of affected individuals

5. Notifying the ICO

5.1. UK GDPR and the Data Protection Act 2018 make it mandatory for serious data breaches to be reported to the ICO.

5.2. Where a breach is likely to result in a risk to the rights and freedoms of natural persons, a notification to the ICO must be made within 72 hours of the Council (not the DPO) becoming aware of the breach. Where a notification to the ICO is not made within 72 hours, it **must** be accompanied by written reasons for the delay.

5.3. The Notification needs to:

(a) Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned.

(b) Communicate the name and contact details of the DPO or other contact point where more information can be obtained.

(c) Describe the likely consequences of the personal data breach.

(d) Describe the measures taken or proposed to be taken by the Council to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

5.4. If it is not possible to provide all the above information at the same time, it may be provided in phases without undue further delay.

The Council is required to record the following information in relation to a personal data breach:

(a) the facts relating to the breach,

(b) its effects, and

(c) the remedial action taken.

It must be recorded in such a way as to enable the ICO to verify compliance.

5.5. Notifying data subjects affected by the breach

The Council is also required to communicate a breach to the affected individuals where the breach is likely to result in a high risk to the rights and freedoms of natural persons.

5.6. The threshold for notifying individuals is set at a higher risk level than that for notification to the ICO.

5.7. Where a breach poses a high risk, the Council should communicate the personal data breach to the data subject without undue delay. This decision should be taken in consultation with the Council's DPO.

5.8. The communication shall include in clear and plain language:

(a) a description of the nature of the breach

(b) the name and contact details of the DPO or other contact point where more information can be obtained.
(c) the likely consequences of the personal data breach.
(d) the measures taken, or proposed to be taken, by the Council to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

5.9. **Circumstances where notification of the data subject is not required**:

- When the data is protected, measures that render personal data unintelligible or inaccessible to any person who is not authorised to access it.
- Immediately following a breach, the Council has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise.
- It would involve disproportionate effort to contact individuals, for example where their contact details have been lost as a result of the breach or are not known in the first place. Instead, the Council must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner.

5.10. The Council may restrict, wholly or partly, the provision of information to the data subject by way of notification to:

- avoid obstructing an official or legal inquiry, investigation, or procedure.
- avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties.
- protect public security.
- protect national security.
- protect the rights and freedoms of others.

6. Review Process

6.1 This policy will be reviewed every two years.

7. Appendix: Breach reporting form (which is available on the Council's intranet)

Reporting Officer:			
Team:			
Service Area & Name of Service Manager			
Directorate			
Date of Breach			
Date Breach Discovered			
Date Breach Reported to DPO			
Please provide a brief explanation for any delay the breach being discovered and for any delay in notifying the DPO			
Does the breach involve Sensitive Personal data	YES	NO	UNKNOWN AT TIME OF REPORTING
Does the breach involve Card Data	YES	NO	UNKNOWN AT TIME OF REPORTING
Description of breach (What caused it, what data was affected, what was/is the impact of the breach			
TO BE COMPLETED BY THE DATA PROTECTION OFFICER:			
RISK ASSESSMENT	HIGH	MEDIUM	LOW
REPORTED TO ICO	YES		NO
DATE REPORTED TO ICO			

IF ICO NOT NOTIFIED RECORD REASON WHY:

DATA SUBJECTS INFORMED	YES	NO
DATE DATA SUBJECTS INFORMED		
IF DATA SUBJECTS NOT INFORMED RECORD REASON WHY:		
DESCRIBE STEPS TAKEN TO REMEDY BREACH /RECOVER DATA OR TO MITIGATE THE RISKS AND IMPACT OF THE BREACH:		
POST BREACH ANALYSIS, FOLLOW UP ACTIONS AND LEARNING POINTS:		

This form is available on the Council's intranet.

A copy of this form or equivalent record will be retained by the Statutory Data Protection Officer in the Data Protection Breach Folder as a record of the London Borough of Hillingdon's handling of, and response to, a data breach incident.