Procedure for Reporting Information Security Breaches, Data Protection Breaches & Card Data Security Incidents

May 2018

Contents

1. Introduction

1.1 This procedure applies to all staff and volunteers working for the Council and it applies to any actual, suspected or "near miss" loss of personal data.

1.2 Any loss of confidential information can result in large fines for the Council. The Council is under a duty to report certain types of breaches so it is imperative that these are reported as soon as possible.

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

1.4 This procedure underpins the Council's information governance policy and related policies which have been developed to protect the information handled by the London Borough of Hillingdon. In addition, it supports the guidelines produced for connecting to the Government Secure Internet and is part of the Council's Payment Card Industry Governance.

1.5 All staff and volunteers have a responsibility to report a suspected or actual breach of confidentiality or loss of data. Failure to do so may be considered a breach of the Council's Data Protection Policy and may result in disciplinary action.

1.6 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.

2. **Procedure**

2.1 If you suspect an information security breach has occurred, you should report it ***immediately*** to the Council's Statutory 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 ralagh@hillingdon.gov.uk. Telephone Number: 01895250617

2.3 The DPO will conduct an initial investigation and risk assessment to ascertain the nature and seriousness of the incident. It is imperative that this assessment is done without delay.

2.4 If a breach meets the notification requirements, the DPO shall inform the Chief Executive of this fact and shall also inform the Information Commissioner

as soon as possible and no later than 72 hours from the time the Council became aware of the breach (see section 4.3 - notification of a breach).

2.5 The DPO does not need to have full details of the breach available prior to making a notification to the Information Commissioner's Officer (ICO). If the DPO believes, on initial assessment, that there is a likelihood that the breach will meet the notification requirements then the DPO should 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 and will implement any recommendations through the Hillingdon Information Assurance Group (HIAG).

3. Breach Management Team

3.1 The Council's DPO will, if he considers 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 effected service area(s). The makeup 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 well-known 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 the GDPR introduces the obligation to notify a breach, it 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.

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.

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.

When the breach involves sensitive 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.

Factors to take into account:

- 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

4.3 Notification of a personal data breach

4.3.1 **Notifying the ICO**

The GDPR and Data Protection Act 2018 makes it mandatory for serious data breaches to be reported to the ICO.

Where a breach is likely to result in a risk to the rights and freedoms of natural persons, a notification to the ICO should 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 shall be accompanied by written reasons for the delay.

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.

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.

4.3.2 **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.

This is a higher risk level than notification to the ICO.

Where a breach poses a high risk, the Council should communicate the personal data breach to the data subject without undue delay.

The communication shall describe 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.

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

(a) When the data is protected, measures that render personal data unintelligible or inaccessible to any person who is not authorised to access it.
(b) 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.
(c) It would involve disproportionate effort to contact individuals, perhaps 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.

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

(a) avoid obstructing an official or legal inquiry, investigation or procedure;
(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
(c) protect public security;
(d) protect national security;
(e) protect the rights and freedoms of others.

Appendix 1 - Breach Reporting Form			
Reporting Officer:			
Team:			
Service Area & Name of Service Manager			
Department			
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 DPA			
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	YES	NOI
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 should be completed in conjunction with the Procedure for Reporting Information Security Breaches, Data Protection Breaches & Card Data Security Incidents

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

Appendix 2

Card Data Security Incident Response plan

May 2018

Contents

1. Scope

1.1. This plan applies to all staff and contractors working for the Council.

2. Purpose

2.1 To address cardholder data security, the major card brands (Visa, MasterCard, etc) jointly established the PCI Security Standards Council to administer the Payment Card Industry Data Security Standards (PCI DSS) that provide specific guidelines for safeguarding cardholder information. One of these guidelines requires that merchants document an incident response plan.

2.2 Any compromise of cardholder data can result in large fines for the Council and damaged reputation. All staff have a responsibility to protect cardholder data.

2.3 This procedure should be used to report all incidents whether actual or suspected. This covers information held and shared in different formats (paper, electronic or verbal).

2.4 The procedure underpins the Council's Information Governance Policy and related policies which have been developed to protect the information handled by the London Borough of Hillingdon.

2.5 A data compromise, or breach, occurs when a person accesses the Council's customer's information with the intent to commit fraud. The information most valuable to criminals include the customer's card number, expiry date, name, address and the security details such as CVC code and the track data. A cardholder data compromise is any situation where theft or suspected theft of cardholder data has occurred.

2.6 Criminals may access cardholder data in a number of ways including:

- Theft from premises of terminals and terminal receipts,
- A dishonest member of staff accessing and passing on cardholder data to criminals,
- A criminal tampering with a card terminal and skimming data,
- Through the Council's third party payment providers.

3. Procedure

2.1 If you suspect an information security breach has occurred, you should report it immediately to your line manager and your service manager.

2.2 If a card terminal has (or is suspected to have been) tampered with, unplug the device and Contact the ICT service desk*. They will alert the IT security team who will collect the terminal and seal it in an evidence bag. ICT can provide spare CAPITA terminals and the Control Accounting Team can arrange for a replacement Global Pay terminal (contact details below).

**The ICT Service desk have completed forensic awareness first responder training.*

2.3 Service managers must report the incident to:

- the Council's SIRO (Senior Information Risk Officer), Muir Laurie. mlaurie@hillingdon.gov.uk, x6132.
- and the Control Accounting Team, Annette Reeves. areeves@hillingdon.gov.uk, x7400.

2.4 The Control Accounting Team will immediately inform the Relationship Manager for the Council's Merchant Services Provider and ensure the payment brands are advised within the necessary timescales. If a card terminal has been stolen or compromised, the Control Accounting team will follow the UK Cards Association procedures.

2.5 The Control Accounting Team will inform the Council's:

- Statutory Data Protection Officer, Raj Alagh. ralagh@hillingdon.gov.uk, ext 0617 who will liaise with the:

- ICT Service

and instigate any necessary remedial action. The Council's Statutory Data Protection Officer will maintain a record of incidents, the outcomes and any recommendations made.

2.6 The Hillingdon Information Assurance Group will review the outcomes of information security breaches and will use the learning to make recommendations to the Corporate Management Team to minimise the likelihood of future recurrence.

4. In Addition

4.1 To minimise further data loss, and preserve evidence to facilitate the investigation process, the Council will not:

- Access, alter or delete files in the compromised system(s).
- Attempt to change passwords on the compromised system(s).
- Log in as ROOT - indeed log on at all.
- Turn (back) on the compromised system(s).

Thus any compromised system(s) will remain in a sealed evidence bag in keeping with LB HIllingdon first responder processes.

- Any logs generated are kept for at least six months in keeping with HMG GPG13.

4.2 While no system is 100% secure, LB Hillingdon:

- Carry out active scans for credit and debit card data on any data stored and transmitted via email, and prevent this from onwards transmission.
- Have controls on USB's being added to computers which makes the movement of skimming of data more difficult from Council computer systems.
- Ensure all permanent staff are vetted to Cabinet Office BPSS v4 standard in terms of eligibility to work and with regard to references on capability and character.
- Employ a Qualified Security Assessor to undertake quarterly scans.
- Only employ 3rd party payment providers who are PCIDSS compliant and listed on the Visa Europe Member or Merchant Agent Weblisting.
- Ensure staff are trained in awareness in relation to card terminal tampering.
- Have specific technical controls in place within the Contact Centre as well as governance and training in relation to processing card payments.