Security Incident and Data Breach Policy

If printed, copied, or otherwise transferred from the Policies and Procedures Intranet/Internet Site this document must be considered to be an uncontrolled copy.

Policy amendments may occur at any time and you should consult the Policies and Procedures Intranet/Internet Site if in doubt.

www.lbbd.gov.uk

Document Control

Title	Security Incident and Data Breach Policy
Document Type	Approved
Author	Information Governance Manager/Data Protection Officer
Owner	SIRO
Subject	Security Incident and Data Breach
Government Security Classification	Official
Created	December 2017
Approved by	Assurance Group
Date Approved	20 April 2018
Review Date	May 2019 or earlier where there is a change in the applicable law or a Council restructure affecting this Policy Guidance

Version Control

Version	Date	Author	Description of Change
1	11/12/17	Yvonne Mason, Information Governance Manager/DPO	New Policy Draft
1.1	14/03/18	Yvonne Mason, Information Governance Manager/DPO	Revised. Amendments to Sections 1 and 6
1.2	31/10/18	Kim Starbuck, Information Governance Manager/DPO	Reviewed and updated with contact details and minor changes to language.

1. Introduction

The London Borough of Barking and Dagenham ('the Council') is responsible for protecting the the vast amount of personal information that we process. As custodians of personal data, we have a mandatory duty to ensure that personal data is protected and processed in accordance with the General Data Protection Regulations 2016/679 (GDPR) and the Data Protection Act 2018 (DPA2018). This responsibility also applies to other organisations working on behalf of the Council (including wholly owned companies e.g. Be First and suppliers).

In the event of a security incident it is imperative that immediate, action is taken to minimise the impact on data subjects, and mitigate associated risks. Security Incidents will be logged, and where necessary, investigated, following the Council's Security Incident process.

Failure to process personal information in accordance with the GDPR and DPA 2018, can result in sanctions. For example, up to €20 million or 4% of global turnover for the preceding year (whichever is the greater) in relation to breaches of rights and obligations and up to €10 million or 2% of global turnover for the preceding year (whichever is the greater) imposed for non-compliance regarding Control and Mitigation.

All individuals permitted to access personal data in line with their work duties must comply with this policy and agree to undertake any relevant training that may be appropriate to the role being undertaken. Some departments may also require you to sign a further undertaking relating to the systems or information you will use.

2. Purpose

The purpose of this policy is to ensure a consistent approach to security breach management, throughout the Council. Security incident management is the process of handling security incidents in a structured and controlled way, ensuring they are dealt with:-

- quickly and efficiently
- a consistent approach across the Council
- that any harm to data subjects, and the Council, is minimised as far as possible
- provides for controls and processes to be reviewed, to reduce the likelihood of a recurrence.

3. Scope

This policy applies to all information held by the Council, falling within scope of the data protection legislations, in all formats including paper, electronic, audio, and visual. It applies to all employees of the Council and those working on behalf of the Council who have access to our information.

Schools may choose to adopt this policy but where this is not the case it is expected that they will have their own appropriate policy.

Manager must ensure that their staff are aware of the security incident process. If employees have any queries, they should discuss these with their line manager or the Data Protection Officer (contact details below).

4. Types of security incidents

A data security incident occurs for a number of reasons, for example:

- Loss or theft of data or equipment, on which data is stored i.e. IT equipment or information (laptops, mobiles, devices containing personal data e.g. memory sticks)
- Unauthorised disclosure containing personal information
- Inappropriate access controls, resulting in unauthorised access to data
- Breach of physical building access/security
- Human error e.g. personal information being left in an insecure location, using incorrect email or postal address, uploading personal information to a website
- Unforeseen circumstances such as fire or flood
- Cyber incidents, such as hacking or phishing‘Blagging’ offences where information is obtained by deception

5. Reporting a security incident

This section explains how to report a security incident including a data breach. It is imperative to note that the Council has 72 hours to report a data breach to the Information Commissioner's Office. Failure to report within this period can result in the Council being sanctioned, (e.g. fined).

5.1 The person who discovers/receives a report of a security incident must inform their line manager immediately. If this is not possible, then another appropriate person should be informed. If the incident occurs or is discovered outside normal working hours this should be done as soon as practicable. The person who discovered the security incident or the manager MUST then report the security incident to the Data Protection Officer immediately by email, and certainly no later than 24 hours using the security incident form (appendix A).

5.2 The Data Protection Officer will determine and lead on an investigation although others may be requested to assist, depending on the severity of the security incident. Employees must not attempt to conduct their own investigations (other than reporting the incident to their Manager and Data Protection Officer.

5.3 The Council's Senior Information Risk Owner (SIRO) and the relevant director are ultimately responsible for making any decisions on serious security and incident breaches.

5.4 Any decision to take disciplinary action will be in line with the Council's disciplinary policy.

5.5 The security incident report will be concluded when all investigations are complete. Assurance Group will be informed and an annual report on incidents will be presented to the Council's Audit & Standards Committee.

6. Responsibility of Data Protection Officer

6.1 Breach Management Plan

The Data Protection Officer will lead all data breach investigations and will follow the Information Commissioner's Office (ICO) suggested Breach Management Plan:-

- Containment and Recovery
- Assessment of ongoing risk
- Notification of Breach
- Evaluation and Response

6.2 Containment and Recovery

Containment and recovery involves limiting the scope and impact of the data breach including, where necessary, damage limitation.

The Data Protection Officer will:

- Lead the investigation

- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a process, finding a lost piece of equipment, or simply changing access codes etc.
- Establish if there is anything that can be done to recover any losses and limit the damage the breach can cause.
- Where appropriate inform the ICO within 24 - 72 hours and;
- Where appropriate inform the police

6.3 **Assessing the risks**

The next stage of the management plan is for the Data Protection Officer to assess the risks which may be associated with the breach considering the potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

In making this assessment the Data Protection Officer will assess:

- What type of data is involved
- How sensitive it is
- If data has been lost or stolen are there any protections in place such as encryption
- What has happened to the data
- What are the consequences if a third party has the data
- How many and who are the individuals' affected
- What harm can come to those individuals
- If there are wider consequences to consider such as a risk to public health or loss of public confidence

6.4 **Notification**

The Data Protection Officer will decide whether the Information Commissioner's Office (ICO) or the data subjects should be notified of the breach and will inform the SIRO. The ICO must be notified within 24 – 72 hours. This is the sole responsibility of the Data Protection Officer and Directorates **must not** make any notifications directly.

The ICO will need to be notified of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals, for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. This will be assessed on a case by case basis by the Data Protection Officer.

6.5 **Evaluation and Response**

The Data Protection Officer will:

- fully review both the causes of the breach and the effectiveness of the response to it
- keep a breach log
- report to the Assurance Group

- implement an action plan to correct identified issues if required
- monitor staff awareness of security issues and look to fill any gaps through training

7. Data Protection Officer Contact Details

Kim Starbuck
Telephone: 0208 227 2061
Email: dpo@lbbd.gov.uk

8. Policy Review

This policy will be reviewed annually, unless changes to legislation, guidance, codes of practice or commissioner advice requires the policy to be updated in addition to the annual review.

Appendix A

Security Incident and Data Breach Notification Form

Contact Details of person submitting form:

Name:	
Job Title:	
Department:	
Contact Number:	
Email:	

Incident Information

Date of incident?	
How did the incident happen?	
Who reported the incident?	
Description of Breach:	

Type of Breach:

Loss of IT equipment	☐	Human error	☐
Theft of IT equipment	☐	Hacking	☐
Unlawful disclosure	☐	Blagging/Phishing	☐
Unlawful access	☐	Fire/Flood	☐
Other *(please describe)*			

Personal data placed at risk

What personal data has been placed at risk? *Please specify if any financial or sensitive personal data has been affected and provide details of the extent.*

Number of Individuals affected: ☐

Have the affected individuals been made aware: Yes ☐ No ☐

What are the potential consequences and adverse effects on those individuals?

Have any affected individuals complained about the incident? Yes ☐ No ☐

Provide details of any action taken to minimise/mitigate the impact on the data subjects.

Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

Please provide brief details of any supporting information:

Details of any contractors/sub-contractors involved: *(if applicable)*

Once completed please email form to:
Data Protection Officer: dpo@lbbd.gov.uk