Data Incident Procedure

Spelthorne Borough Council holds large amounts of personal data, including special category personal data. Every care is taken to protect personal data and to avoid a data protection breach.

Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs.

Purpose

The Council is obliged under Data Protection legislation to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility. This document sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the Council. This document relates to all personal and special categories (sensitive) data held by the Council regardless of format.

The Council recognises that from time to time 'things go wrong' and there may be a breach of security involving information or equipment holding personal information. The purpose of reporting an incident is not to apportion blame but to ensure that any impact is minimised and lessons learnt can be identified and disseminated.

The purpose of this procedure is to ensure that all actual or potential information security incidents are reported centrally to enable the Council to react quickly and effectively to minimise the impact.

The aims of the procedure are as follows:

• Timely advice on containment and risk management
• Determine whether further controls or actions are required
• Evaluate lessons learnt and areas for improvement

All information security incidents will be dealt with by the Data Protection Officer (DPO), with the Senior Information Risk Officer providing cover in the absence of the DPO.

This procedure applies to all employees, councillors, agency staff, contractors or any other persons who have access to, or use the Council's information.

Types of Incident
There is no simple definition of an information security incident but generally it will involve an adverse event which results, or has the potential to result in the compromise, misuse or loss of SBC owned or held information or assets.

Such incidents could be caused by a number of factors. Some examples are:

- Loss or theft of personal data and/ or equipment on which data is stored;

- Inappropriate access controls allowing unauthorised use;

- Equipment Failure;
- Human Error;
- Unforeseen circumstances such as fire or flood;
- Hacking;
- 'Blagging' offences where information is obtained by deception.

Broadly speaking a data breach is a breach of security that compromises the Confidentiality, Integrity or Availability of personal data.

Incident Reporting:
The impact of a security incident can vary greatly depending on the type of information or asset involved. It may for instance lead to an infringement of privacy, fraud, financial loss, service disruption or reputational damage.

The person who discovers/receives a report of an incident must inform the Data Protection Officer or, in their absence, either the Senior Information Risk Officer (Group Head of Commissioning & Transformation) or their deputy within 24 hours. All information security incidents must be reported to data.protection@spelthorne.gov.uk.

Immediate Containment/Recovery
Steps must be taken immediately to minimise the effect of the breach, these could include:

- Recovery of any equipment,
- Changing passwords,
- Containment by asking recipients to delete inappropriately shared personal data

A direct line manager or supervisor should always be made aware of any information security incident.

Any incidents involving lost or stolen equipment or a network security issue should be reported to the ICT Service Desk. For the purposes of this procedure lost or stolen hardware will be logged and may be subject to further investigation depending on the circumstances giving cause to the incident. The Police should be notified immediately of any incidents involving stolen information or equipment and a crime reference number obtained.

For other incidents the SIRO must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

Incident Assessment:
The DP Officer will assess the incident including an assessment of any risks to ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps, further to immediate containment, need to be taken to recover any losses and limit any damage.

Notification
Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to comply

with the requirement that data controllers notify the Information Commissioner's Office significant breaches.

Incident Report:
Not all incidents will require an in depth investigation to establish the facts and determine what occurred. The DPO may fully investigate the breach to ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections are in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (customers, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record will be made of the nature of the breach and the actions taken to mitigate it. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Review and Evaluation

Once the initial aftermath of the breach is over, the SIRO (or nominated representative) will fully review both the causes of the breach and the effectiveness of the response to it.

This document will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation. This document was last reviewed in December 2018.