Data Breach Policy

Last updated May 2023

Contents

Document Control

Version	Date	Reason for Change	Amended by
1.0	03/23	Creation of document.	Head of ICT
1.1	12/04	Reviewed by Director of Governance.	Director of Governance
1.2	01/05	Approved by SMT.	Head of ICT

Next Review Date: March 2024

This policy applies equally and jointly to each authority, however the data will be processed locally.

1. Purpose and Scope

The Council stores, processes, and shares a large amount of personal information. Data is a valuable asset that needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidentally or deliberately). Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage or detrimental effect on the Council.

We are obliged under the Data Protection Act and the GDPR to have a process in place designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility. This policy 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.

This Policy recognises that whilst personal and sensitive data is processed by the Council it is owned by the individual to whom it relates, and this must be considered in any decision making by the Council.

This Policy relates to all personal and sensitive data held by the Council Regardless of format.

This Policy applies to everyone at the Council. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the Council.

The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

2. What is a data breach?

For the purpose of this Policy, data security breaches include both confirmed and suspected incidents. An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately.

An incident includes but is not restricted to, the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record).

- Equipment theft or failure.

- Unauthorised use of, access to or modification of data or information systems.

- Attempts (failed or successful) to gain unauthorised access to information or IT system.

- Unauthorised disclosure of sensitive/confidential data.

- Website defacement.

- Hacking attack.

- Unforeseen circumstances such as a fire or flood.
- Human error.

- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

3. How do I report a breach?

Any individual who accesses, uses or manages information is responsible for reporting data breach and information security incidents immediately to the appropriate manager and the Head of ICT.

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable. The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process. All staff should be aware that any breach may result in disciplinary procedures being instigated.

4. Containment and Recovery

Appropriate steps must be taken immediately to minimise the effect of the breach. An initial assessment will be made to establish the severity of the breach and to establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The investigation will need to take into account the following:

- The type of data involved.

- Any sensitivity for example information relating to children/vulnerable adults.

- The protections that are in place (e.g. encryptions).

- What's happened to the data, has it been lost or stolen.

- Whether the data could be put to any illegal or inappropriate use.

- Who the individuals are, number of individuals involved and the potential effects on those data subject(s).

- Whether there are wider consequences to the breach.

5. Notification

Management should determine who needs to be notified of the breach. Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- Whether there are any legal/contractual notification requirements.

- Whether notification would assist the individual affected – could they act on the information to mitigate risks.

- Whether notification would help prevent the unauthorised or unlawful use of personal data.

- Would notification help the Council meet its obligations under the seventh data protection principle.

- If a large number of people are affected, or there are very serious consequences.

- Whether the Information Commissioner's Office (ICO) should be notified. The ICO will only be notified if personal data is involved and this should be within 72 hours of becoming aware of the breach.

Failing to notify a breach when required to do so can result in a fine up to £9 million.

All suspected and actual breaches should be recorded for further evaluation and breach avoidance activity.

Not every incident however, warrants notification and over notification may cause disproportionate enquiries and work.

Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved.

Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks. Individuals will also be provided with information on what has occurred.

6. Evaluation and response

Once the initial incident is contained, the organisation will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls should be reviewed to determine their adequacy and whether any corrective action should be taken to minimise the risk of similar incidents occurring.