City of Bradford Metropolitan District Council

City of Bradford Metropolitan District Council

- Data Security Incident Policy

1. Background

Data security incidents are increasingly common occurrences whether caused through human error or via malicious intent and as the amount of data and information grows and technology develops, there are new ways by which personal data can be breached.

The Council needs to have in place a robust and systematic process for responding to any reported data security incident, to ensure it can act responsibly and protect the personal data it holds.

2. Definition

Article 4 (12) of the General Data Protection Regulation ("GDPR") defines a personal data security breach as:
"A breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

A personal data security breach can come in many forms, but the most common are as follows:

- Loss or theft of paper or other hard copy data
- Data posted, e-mailed or faxed to the incorrect recipient or address
- Loss or theft of equipment on which data is stored that is not appropriately encrypted.
- Inappropriate sharing or dissemination of data
(*e.g. staff accessing information to which they are not entitled or enclosed with a bundle of documents*)
- Hacking, malware, data corruption
- Information obtained by deception or "blagging"
- Equipment failure, fire or flood
- Unescorted visitors accessing data
- Non-secure disposal of data

3. Policy statement

The City of Bradford Metropolitan District Council ('the Council') is committed to fulfilling its obligations under the legislation and to ensuring that where data is misdirected, lost, hacked or stolen, inappropriately accessed or damaged, the incident will be properly investigated and, where necessary, reported to the Information Commissioners Office (ICO), or any other appropriate supervisory authority, and/or the data subject(s) in addition to taking any necessary action to rectify the situation.

The aim of this policy is to standardise the Council's response to any personal data breach and to set out how the Council will manage reports of suspected data security incidents.

In summary the Council will ensure that all data security incidents are;-

- Reported swiftly so that they can be properly investigated
- Appropriately logged and documented
- Dealt with in a timely manner and normal operations restored

- Risk assessed to ensure that the impact of the incident is understood, and action taken to prevent further damage
- Appropriately reported to the ICO, affected data subjects informed or any other appropriate supervisory authority (as is required in more serious cases)
- Reviewed, and lessons learned
- Managed in accordance with the law and best practice.

4. Scope

This policy applies to all Council information, in both paper and electronic format, and is applicable to all employees, members, visitors, contractors, partner organisations and data processors acting on behalf of the Council and should be read in conjunction with any other Information Security Policies.

5. Reporting an incident

a) Internal reporting

All suspected data security incidents must be reported to the Corporate Information Governance team, **within 24 hours** of the suspected incident occurring or of the suspected incident being discovered.

Reports must be made by completing the online form. Non PC Users should telephone the Corporate Information Governance team on 01274 434506 with the details of the incident.

Where the security of the Council's IT network may have been seriously compromised then these incidents should be reported to the IT Contact Centre on 01274 431234 immediately.

The Corporate Information Governance team will maintain a central log of all reported incidents to ensure appropriate oversight, in the types and frequency of confirmed incidents, for management and reporting purposes and all documentation on personal data breaches, including the facts, and any remedial action taken, will be maintained.

Any personal data where there is a likelihood that it may result in "a risk to the freedoms and rights of natural persons" must be communicated, to both the ICO and the data subject (with certain exceptions), "without undue delay" and within 72 hours of becoming aware of it. If the council fails to do this, it must explain the reason for the delay. The Corporate Information Governance team will be responsible for notifying the ICO.

b) External reporting

All suspected data security incidents can be reported to the Corporate Information Governance team by completing the online form available on the Council's website www.bradford.gov.uk or by telephoning the Corporate Information Governance team on 01274 434506.

6. Data Breach Management Plan

The Council's response to all reported personal data security breaches will consider the following four elements.

1. Containment and Recovery
2. Assessment of Risks
3. Consideration of Further Notification
4. Evaluation and Response including any organisational learning to prevent possible future occurrence.
5. Recording/Evidence of actions taken

7. Responsibilities

All Council employees (including members, visitors, contractors and data processors, acting on behalf of the Council) are responsible for;-

- The immediate reporting of actual, suspected, threatened or potential data security incidents as soon as they are known and for assisting with any subsequent investigation as required, including taking action required to prevent further damage.

All line managers are responsible as **"Incident Owners"** for;-

- Notifying the Corporate Information Governance team and the Service Information Asset Owner, **within 24 hours**, of any actual, suspected, threatened or potential information security incidents.
- Carrying out an investigation into what has happened including determining what, if any personal data is involved and documenting actions.
- Taking action to prevent further damage.
- Notifying the Corporate Information Governance team of the outcome of the investigation and deciding on the next course of action.

Information Asset Owners (Directors/Assistant Directors) are responsible for;-

- Ensuring that all employees, within their service area, understand their responsibilities and comply with this policy.

Corporate Information Governance Officers are responsible for**;-**

- Assessing reported data security incidents to establish whether there has been a personal data breach. (Reported incidents where there has not been a personal data breach will be logged and forwarded to IT Services to action (see below).
- Collecting any additional information from Services on the personal data breach as appropriate.
- Carrying out a risk assessment to establish the severity of the breach.
- Liaising with the Incident Owner as to further action.

IT Services staff are responsible for;-

- Taking appropriate action on all reported security incidents involving the Council's IT systems and/or equipment.

Data Protection Officer is responsible for;-

- Overseeing the management of all personal data breaches to ensure that they have been actioned in accordance with the Council's Data Breach Management Plan (See para 6 of this policy) and the legislation, referring any non compliance to the Senior Information Risk Owner.
- Reporting to the ICO, or any other appropriate supervisory authority

8. Non compliance with this policy

Employees, members, contractors, visitors or partner organisations who act in breach of this policy may be subject to disciplinary procedures or other appropriate sanctions.

9. Review

This policy will be subject to annual review by the Council's Information Assurance Group.