Data Protection Breach Management Plan

Adopted at the Full Council Meeting held on 23rd May 2024

General

The purpose of the Data Protection Breach Management Plan is to ensure a standardised approach in the reporting, containment and management of a breach involving personal data.

A breach, loss or compromise of personal data may be the result of either:

- Loss or theft of equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Human error;
- Unauthorised disclosure;
- Accidental destruction;
- Hacking or targeted attack;
- Unforeseen circumstances such as fire/flood.

Control

In the event of a breach:

- Advise Data Controller Officer
- Explain what happened, why it happened and method of dealing with the breach
- Data Controller Officer will decide if the ICO needs to be informed

Action

It is important to take immediate action to help reduce harm and distress to data subjects and limit damage. It is also important to identify trends and improve policy, processes and procedures to prevent recurrence.

- A breach, loss or compromise of personal data, no matter how small in scale, is to be reported to Data Controller Officer immediately.

- A data protection breach will require not just an initial response, but also containment and recovery including where necessary, damage limitation. It is important to establish quickly whether there is anything that can be done to recover any losses and limit the scope of further damage the breach has or could cause. Activities could include isolating or closing social media sites, finding lost equipment or documents or changing access codes to a secure cabinet or office.

- Assess the risk to data subjects and the council's reputation resulting from the breach. Some data security breaches will not lead to risks beyond inconvenience to those who need the data to carry out their job, an example might be where a pc is irreparably damaged but its files were backed up and can be recovered. While these types of incident can still have significant consequences the risks are very different from those posed by the loss or compromise of Category A and B (see annex A) personal data which may be used to commit identity fraud.

- Notification can be an important element of breach management strategy. It should have a clear purpose, for example to enable affected data subjects to take steps to protect themselves or allow appropriate regulatory bodies to take action and/or provide advice. The decision to notify a data subject of a breach, loss or compromise is to be taken on a case by case basis.

Lessons and Closure

It is important to evaluate the effectiveness of the response to a breach and learn/identify lessons.

For example, a review of policies, processes and procedures may be necessary to ensure continuous improvement and avoid the situation arising again.

- Identify weakness in existing policy, processes and procedures
- Is a review of the Data Protection Policy necessary to improve processes and procedures in the processing of personal data?
- Establish where the greatest risks lie; for example how much personal data is held and where is it stored.
- Ensure the method of transmission used when sharing or disclosing personal data to others is secure and only the minimum amount of data necessary to achieve output/service is disclosed. By doing this, in the event of a breach, risk will be reduced.

Annexes:

A. Personal, Protected and Sensitive Personal Data

Annexe A

PERSONAL, PROTECTED AND SENSITIVE PERSONAL DATA

(Note: the below lists are not inclusive)

Category A – Personal Data. Example:

- Name
- Work/Business Address
- Work/Business Email
- Postcode
- Telephone numbers
- Date of Birth
- Identifiable Photograph

Category B – Protected Personal Data. Example:

- Pay, banking or financial details
- National Insurance Number
- Passport Number
- Driving License Number
- Performance Reporting
- Next of Kin/Family Details (spouse/partner/children)
- Home Address
- Home Email
- Medical Information
- Education/Qualification Details
- Welfare Information, such as material relating to social services/child protection/housing
- Tax, benefit or pension records
- Nationality
- CCTV

Category C – Sensitive personal Data. Example:

- Sexual/gender matters
- Physical or mental health condition
- Religious beliefs or beliefs of a similar nature
- Political opinions
- Racial or ethnic origin
- The commission or alleged commission of any offence
- Any casework or record relating to any offence committed or alleged to have been committed, any proceedings and the disposal of such proceedings or the sentence of any court.
- Membership of a trade union
- DNA or fingerprints
- Free text boxes (embedded within applications/forms)

Document History			
Version	**Issued**	**Reviewed**	**Approved**
Draft			
1			