CODE OF PRACTICE – DATA BREACHES

Statement and Purpose

This Code of Practice has been developed to assist the Council in responding effectively to personal data breaches. The Council holds substantial amounts of personal and special categories data and care must be taken to avoid a data breach. In the unlikely event of there being a breach, it is vital that appropriate action is taken as soon as possible to minimise any associated risk.

Legal Context

The GDPR and Data Protection Act 2017 make provision for the regulation of the processing of information relating to individuals including the obtaining, holding, use or disclosure of such information.

The crux of the legislation is that it imposes an obligation on all data controllers to comply with the six data protection principles. The sixth principle deals with security and states that organisations which process data must process data "*in a manner that ensures the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*

The Council must have security measures in place which are appropriate to the harm that could result from a loss of the particular data or its unauthorised processing. In practice, this means that the Council must assess the security options available in light of the potential harm, cost of the security measure, level of sensitivity of the data, and the technology available; different levels of security may be appropriate to different types of data.

Types of Breach

Data Breaches can be caused or exacerbated by a variety of factors, affect different types of personal information and give rise to a range of actual or potential harms to individuals, agencies and organisations.

'Personal Data Breach' for the purpose of this document means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data Breaches occur in a number of ways:

- Lost or stolen laptops or paper records containing personal information;
- Mistakenly providing personal information to the wrong person for example by sending information to the wrong address;
- Human error;
- Hacking;
- Databases being illegally accessed by individuals outside the Council;
- Unforeseen circumstances such as fire or flood

Each breach will be dealt with on a case-by-case basis, undertaking an assessment of the risks involved and using that risk assessment as the basis for deciding what actions to take in the circumstances.

The following key steps must be followed when responding to a breach:

Take immediate steps to limit the breach

- Stop the unauthorised practice, shut down the system, recover the files, change computer access, alert relevant staff.

Escalate the matter as appropriate

- The person who discovers/receives a report of a breach must inform the Data Protection Officer without undue delay. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable

- Consider whether anyone externally needs to be notified (eg if the breach involves criminal activity then notify the police)

Investigation

- The relevant manager must fully investigate the breach. The investigation should consider:
- What type of personal information is involved?
- Who is affected by the breach? Is someone at risk of harm?
- Is there a risk of ongoing breaches?
- What was the extent of the breach?
- Consider whether the personal information is adequately encrypted, anonymised or not easily accessible
- Has the personal information been recovered?
- How many individuals are affected by the breach? (Remember that while the number of affected individuals will help to gauge the severity of the breach, sometimes a breach involving one individual can be very serious)
- Is this an isolated incident or a systemic problem? Consider whether similar breaches have previously occurred.
- What harm could result from the breach? (threat to physical safety, financial loss, identity theft)
- Have appropriate measures been taken to mitigate the possible adverse effects of the breach?

A clear record should be made of the nature of the breach and the actions taken to mitigate it.

Notification

The GDPR introduces a legal duty on organisations to report a serious personal data breach which interferes with the rights and freedoms of the data subject to the ICO within **72 hours** of becoming aware of it. The Data Protection Officer in consultation with legal will determine whether the breach falls into this category.

- The Data Protection Officer will be responsible for notifying the ICO. Notification must include :
- (a) a description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- (b) the name and contact details of the contact point from whom more information can be obtained;
- c) a description of the likely consequences of the personal data breach;
- (d) a description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate measures to mitigate its possible adverse effects.

- Individuals affected by the breach must be notified directly by the relevant line manager as soon as is practicable by phone or in person and this should ideally be undertaken by someone who has a direct relationship with that affected individual where possible (e.g social worker)

Review and Evaluate

- The Head of Service should review the causes of the breach and the effectiveness of the response to it and take any necessary action to prevent future breaches.

- If systematic or ongoing problems are identified, then an action plan must be drawn up to put these rights.

- Appropriate changes to policies, procedures and staff training practices will be undertaken where necessary.

- All breaches will be reported to the Information Governance Board and Corporate Management Board from time to time.