DATA BREACH PROCEDURE

1. Introduction

1.1 The Council has a responsibility to ensure that personal data is processed securely and in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. A personal data breach may occur where personal data is accidentally or unlawfully destroyed, lost, altered, disclosed, or accessed without authorisation.

1.2 All actual or suspected personal data breaches, security incidents, or near misses must be reported immediately to the Council's Data Protection Lead. Prompt reporting enables the Council to assess the incident, take appropriate remedial action, and determine whether notification to the Information Commissioner's Office (ICO) and/or affected individuals is required.

1.3 Not all incidents will result in a reportable breach. However, incidents where personal data has been put at risk, even if no loss or disclosure ultimately occurs, must still be reported so that lessons can be learned and recurrence prevented.

1.4 All councillors, employees, and volunteers who handle personal data must be familiar with and follow this procedure.

2. Reporting a suspected breach

2.1 Any person who becomes aware of a potential personal data breach or security incident must report it as soon as possible to the Data Protection Lead. Where there is uncertainty as to whether an incident constitutes a breach, it should still be reported and assessed.

2.2 When reporting an incident, the following information should be provided where known:

- What happened and when it was discovered
- The nature of the personal data involved
- The approximate number of individuals affected
- Whether the data includes special category data
- Any immediate action already taken

3. Initial assessment and investigation

3.1 The Data Protection Lead will promptly assess the incident to determine:

- Whether it constitutes a personal data breach under UK GDPR
- The likely risk to the rights and freedoms of individuals
- Whether containment or recovery action is required immediately

3.2 The Data Protection Lead will investigate the circumstances of the incident, including its cause, scope, and impact, and will determine appropriate remedial and preventative measures.

3.3 Where appropriate, the Data Protection Lead may obtain statements or information from individuals involved in the incident to ensure an accurate understanding of events.

4. Notification and escalation

4.1 Where a personal data breach is likely to result in a risk to the rights and freedoms of individuals, the Data Protection Lead will ensure that the Information Commissioner's Office is notified without undue delay and, where required, within 72 hours of becoming aware of the breach, in accordance with UK GDPR.

4.2 If notification to the ICO is made after 72 hours, the reasons for the delay will be recorded.

4.3 Where a personal data breach is likely to result in a high risk to individuals, the Data Protection Lead will ensure that affected individuals are informed without undue delay, unless an exemption applies.

5. Incident record and follow-up

5.1 For each reportable incident, the Data Protection Lead will ensure that an internal record is maintained, including:

- A summary of the incident
- Dates and times
- Assessment of risks
- Decisions taken regarding notification
- Actions implemented to mitigate the breach
- Measures identified to prevent recurrence

5.2 The Data Protection Lead will report significant incidents and learning outcomes to the Council as appropriate.

6. Preventative action

6.1 Following investigation, the Council will implement reasonable and proportionate measures to reduce the likelihood of similar incidents recurring. This may include:

- Process or policy changes
- Additional guidance or training
- Technical or organisational controls

7. Templates and correspondence

7.1 Template letters for notifying affected individuals or responding to breach reports may be maintained separately for operational use. Any correspondence will be proportionate, clear, and avoid unnecessary disclosure.

8. Relationship to other policies

8.1 This procedure should be read alongside the Council's:

- Data Protection Policy
- IT and Security Policy
- Retention Schedule

9. Monitoring, Review and Maintenance

9.1 This procedure will be kept under review to ensure it remains effective and compliant with data protection legislation and relevant regulatory guidance.

9.2 The Data Protection Lead is responsible for reviewing this procedure periodically, and at least annually, or sooner where required as a result of:

- changes to legislation or guidance;
- changes to the Council's processing activities; or
- lessons learned from a data protection incident or near miss.

9.3 Any material changes to this procedure will be reported to the Council and implemented as necessary.