HELSBY PARISH COUNCIL

DATA BREACH POLICY

Version 1 - Adopted by Full Council on 9th December 2024
Latest Review by the Policy and Procedures Committee on 25th November 2024
Revision by the Policy and Procedures Committee due: November 2025

1. Introduction and Background

1.1. Helsby Parish Council holds a large amount of information in a variety of formats. This includes personal and sensitive personal data and non-personal information which may be sensitive or commercially confidential.

1.2. The parish council has legal responsibilities to ensure that the information within its control is safeguarded. Care will be taken to protect information, to ensure its integrity and to protect it from loss, theft or unauthorised access.

2. Scope of the Policy

2.1. This policy defines a data breach incident and sets out the parish council's procedures to follow on the reporting of a data breach.

2.2. This document applies to all councillors, committees, employees of the council, contractual third parties and agents of the council who have access to information systems or information used for Helsby Parish Council purposes.

2.3. Any member of the above discovering or suspecting a data breach incident must report it in accordance with this policy.

3. Definition

3.1. A data breach incident is an event which occurs when data or information held by the parish council, in any format, is compromised by being lost, destroyed, altered, copied, stolen, transmitted, unlawfully accessed or used by unauthorised individuals, whether accidently or on purpose.

4. What is Covered by a Data Breach Incident?

4.1. The following is covered:

- The loss or theft of data or information;

- The loss or theft of equipment upon which the data is stored;
- Unauthorised access to data or information storage or computer systems;
- Transfer of data or information to those who are not entitled to receive that information;
- Failure of equipment or power leading to loss of data;
- Environmental – deterioration of paper records;
- Changes to information or data or system hardware, firmware or software characteristics without the council's knowledge, instruction or consent;
- Unauthorised use of a system for the processing or storage of data; and
- Data maliciously obtained by way of social engineering (i.e. an attack in which a user is 'tricked' into giving a third-party access).

5. When to Report the Breach

5.1. All data breaches should be reported immediately to the parish council via the clerk.

5.2. The clerk will require the person reporting the data breach to provide further information, the nature of which will be dependent upon the incident being reported.

5.3. In all types of breaches being reported, the following must be supplied:

- Contact details of the person reporting the breach;
- The type of data or information involved (not the data unless specifically requested);
- Whether the data related to people and if so how many people involved;
- Location of the incident;
- Inventory and location of any equipment affected;
- Date and time the data breach occurred; and
- Type and circumstances of the incident.

5.4. The chair of the parish council will also be informed to enable them to investigate and confirm that the details represent a valid data breach as defined above.

5.5. The parish council is responsible for maintaining a confidential log of all data breach events.

6. Investigation and Response

6.1. The parish council will consider the report, and where appropriate, investigate the circumstances and the effect(s) of the data breach.

6.2. An investigation will be started into material breaches within 24 hours of the breach being discovered, where practical.

6.3. The investigation will cover the nature of the incident, the type of data involved, whether the data is personal data relating to individuals or otherwise confidential or valuable. If personal data is involved, associated individuals must be identified and, if confidential or valuable data is concerned, what the legal and commercial consequences of the breach may be.

6.4. The investigation will also cover the extent of the sensitivity of the data and a risk assessment will be carried out as to what might be the consequences of the loss. This will include damage and/or distress to individuals and the parish council.

6.5. HPC will be responsible for formally recording the incident and the associated response.

7. Escalation and Notification

7.1. The clerk and chair will be responsible for the initial assessment of an incident's severity based on its scope, scale and risk.

7.2. The preliminary decision is then to be reviewed by the full parish council.

7.3. If a personal data breach has occurred of such a scale, the parish council will instruct the clerk as the Proper Officer of the Council to notify the Information Commissioner's Office (ICO) within the prescribed statutory limits. The clerk will manage all communications between the parish council and the ICO.

7.4. If the breach is deemed to be of sufficient seriousness (in line with ICO guidance) and concerns personal data, notice of the breach will be made to affected individuals to enable them to take steps to protect themselves. Such a notice will include a description of the breach and the steps taken by the parish council to mitigate the risks. Liaison with the police and other authorities may be required for serious events.

8. Review

8.1. Once the incident had been contained, HPC will undertake a thorough review of the event to establish the cause of the incident, the effectiveness of the response and will identify the areas that require improvement.

8.2. Any recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.

8.3. Any weaknesses or vulnerabilities that may have contributed to the incident will be identified, and plans put in place to resolve and avoid any future incidents occurring.