HALEBANK PARISH COUNCIL

DATA PROTECTION BREACH POLICY

ADOPTED 8 JUNE 2026

A. Purpose

The council is required under the data protection legislation to have in place a robust breach detection investigation and internal reporting procedure. This policy describes the steps that will be taken to investigate and respond to potential data breaches to minimise the risk of harm to individuals and the reputation of the Council.

B. Scope

What information does the policy apply to? This policy applies to all information held by the Council both in electronic and hard copy format.

C. Understanding and identifying a Data Protection Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. This policy applies to both breach incidents that are confirmed to have taken place and suspected breaches that require appropriate Council staff to investigate the incident.

Examples of incidents that could result in a data protection breach include (but not restricted to):

- Unauthorised disclosure of personal information to external parties (either accidental or deliberate),
- Information sent in error to an unintended recipient.
- Phishing attacks that have resulted in personal information disclosure or disclosure of access details to Council systems.
- Loss or theft of devices on which Council personal data is stored (e.g. laptops and tablets).
- Loss of theft of hard copy materials including personal data.
- Hacking attacks of Council systems.
- Equipment failure resulting in loss of data.

D. Reporting a Confirmed or Suspected Data Protection Breach

All staff are required to act promptly to notify the Council of a suspected breach to ensure that the incident is contained quickly. The Parish Clerk will inform the IT providers of the incident.

Staff involved need to ensure they respond to further requests for information as soon as possible whilst activity takes place to understand the risk from the incident reported.

E, Incident Investigation

For breaches resulting from IT security-based incidents the investigations will be led by appropriate staff. The Parish Clerk will lead non-IT security-based incidents investigations.

If a breach is confirmed to have occurred the Council will take action:

- Ensure all appropriate steps are taken to contain the breach.
- Ensure affected data subjects have been notified where appropriate.
- Create a record of the incident.
- Asses if all staff training or procedures require improvement to prevent repeat incidents.
- Assess if any system security issues need to be strengthened.
- Investigate whether individual staff should be subject to any disciplinary action in the event of serious breaches resulting in poor adherence to expect standard.

F. Incident reporting to the ICO

The Council will act to comply with data protection legislation to notify the ICO of reportable incidents with the required timescale of 72 hours from being aware of the breach. The Council will assist the ICO as required. This action will be led by the Parish Clerk and reported to the Council. Other staff may be required to support this activity and will be expected to comply with this without delay.

G. Breach register

On completion of the investigation the Parish Clerk will update the Council's data protection breach register to record the details of the incident and action taken.

H. Evaluation and review

This policy will e formally review every year by the Parish Clerk. In addition, the effectiveness of this policy will be monitored as necessary on an on-going basis to ensure that it Is compliant with relevant legislation.