

Helpringham Parish Council

Data Breach Policy

Adopted: 19/8/26

Minute ref: 76/27

Review: July 2027

UK GDPR defines a personal data breach as “a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data whether electronic or hard copy.

Examples include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data
- Unauthorised access through cyber attack, phishing, malware or compromised passwords.

Helpringham Parish Council takes the security of personal data seriously, computers are password protected and hard copy files are kept in locked cabinets.

Consequences of a personal data breach

A breach of personal data may result in a loss of control of personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data, damage to property or social disadvantage. Therefore a breach, depending on the circumstances of the breach, can have a range of effects on individuals. The Council must assess the level of risk to individuals as part of its breach response process.

Helpringham Parish Council's duty to report a breach

If the data breach is likely to result in a risk to the rights and freedoms of the individual, the breach must be reported to the individual and ICO without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. The Data Protection Officer must be informed immediately so they are able to report the breach to the ICO in the 72 hour timeframe.

If the ICO is not informed within 72 hours, Helpringham Parish Council via the DPO must give reasons for the delay when they report the breach.

The Council must also document all decisions made during the breach handling process, including justifications for reporting or not reporting.

When notifying the ICO of a breach, Helpringham Parish Council must:

- Describe the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
- Communicate the name and contact details of the DPO
- Describe the likely consequences of the breach
- Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse affects.
- Provide any additional information requested by the ICO during the investigation.

When notifying the individual affected by the breach, Helpringham Parish Council must provide the individual with (ii)-(iv) above. The Council must communicate in clear, plain language and provide on how individuals can protect themselves.

Helpringham Parish Council would not need to communicate with an individual if the following applies:

- It has implemented appropriate technical and organisational measures (i.e. encryption) so those measures have rendered the personal data unintelligible to any person not authorised to access it;
- It has taken subsequent measures to ensure that the high risk to rights and freedoms of individuals is no longer likely to materialise, or
- It would involve a disproportionate effort

However, the ICO must still be informed even if the above measures are in place.

When communication would involve disproportionate effort, the Council must make a public communication or similar measure to inform affected individuals.

Data processors duty to inform Helpringham Parish Council

If a data processor (i.e. payroll provider) becomes aware of a personal data breach, it must notify Helpringham Parish Council without undue delay. It is then Helpringham Parish Council's responsibility to inform the ICO, it is not the data processors responsibility to notify the ICO.

All processor contracts must include mandatory UK GDPR breach notification clauses.

Records of data breaches

All data breaches must be recorded whether or not they are reported to individuals. This record will help to identify system failures and should be used as a way to improve the security of personal data.

The council must maintain a Data Breach Log and review it annually as part of governance and audit requirements under the English Devolution and Community Empowerment Act 2026.

Record of Data Breaches

Date of breach	Type of breach	Number of individuals affected	Date reported to ICO/individual	Actions to prevent breach recurring

To report a data breach use the ICO online system:

<https://ico.org.uk/for-organisations/report-a-breach/>

The Council must follow its internal Data Breach Response Procedure.