

The Parish Council of Little Harrowden



Clerk: Sylvia Tilaks
Mulberry Cottage
15 Main Road, Grendon, NN7 1JW

Telephone 07942 292479
Email: clerk@littleharrowdenparishcouncil.gov.uk
<https://littleharrowdenparishcouncil.gov.uk/>

Data Breach Policy

Procedure reviewed and adopted at the meeting of Little Harrowden Parish Council held on: 10.05.23

Updated and adopted: 9th September 2026

Signed:

Name:

Position:

Date:

Data Breach Policy

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 transmitted, stored or otherwise processed”.

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

Little Harrowden Parish Council takes the security of personal data seriously and implements appropriate technical and organisational measures proportionate to the risks associated with the personal data it processes. These include, where appropriate, password protection and access controls, secure storage of paper records, appropriate security of electronic devices and systems, secure disposal and appropriate backup and recovery arrangements.

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.

Action following discovery of a breach

Any councillor, employee, contractor or other person acting on behalf of the Council who becomes aware of an actual or suspected personal data breach must report it immediately to the Clerk and the Council's Data Protection Officer (where applicable).

The Council will, as appropriate:

- Take immediate action to contain the breach and prevent further loss or disclosure
- Establish when the breach occurred and when the Council became aware of it
- Identify the personal data and individuals affected
- Investigate the cause and circumstances
- Assess the likelihood and severity of the risk to individuals' rights and freedoms
- Determine whether notification to the ICO and/or affected individuals is required
- Document the breach, risk assessment and decisions taken
- Identify and implement any remedial or preventative action required

Little Harrowden 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 individuals, the breach must be reported to the ICO without undue delay and, where feasible, not later than 72 hours after Little Harrowden Parish Council has become aware of the breach. Where the breach is likely to result in a high risk to the rights and freedoms of individuals, the Council must also inform the affected individual(s) without undue delay. The Clerk and the Council's Data Protection Officer (where applicable) must be informed immediately so that the breach can be assessed and, where required, reported within the 72 hour timeframe.

If the ICO is not informed within 72 hours, Little Harrowden Parish Council must give reasons for the delay when it reports the breach.

If all relevant information is not available within the 72-hour period, the Council will make an initial notification using the information available and provide further information to the ICO without undue delay as it becomes available.

1. When notifying the ICO of a breach, Little Harrowden 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 or other contact where more information can be obtained
 - 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 effects.
2. When notifying an individual affected by a breach that is likely to result in a high risk to their rights and freedoms, Little Harrowden Parish Council must describe the nature of the breach in clear and plain language and provide the individual with the contact details, likely consequences and measures described above.
3. Little Harrowden 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. In such a case, the Council must instead make a public communication or take a similar measure whereby the individuals are informed in an equally effective manner.

Whether the ICO must be notified is determined separately in accordance with the reporting threshold above. Where the Council decides that a breach does not require notification to the ICO, the breach and the reasons for that decision must still be recorded. To report a data breach use the ICO online system: <https://ico.org.uk/for-organisations/report-a-breach/>

Data processors duty to inform Little Harrowden Parish Council

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

Contracts with data processors must require them to notify the Council of a personal data breach without undue delay and to provide the information and assistance reasonably required by the Council to investigate, assess and respond to the breach.

Records of data breaches

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

Record	Details to include
Date and circumstances	Date/time discovered; when/if the breach occurred; brief details of what happened.
Data and people affected	Type of personal data involved and approximate number/type of individuals affected.
Risk and impact	Actual or potential consequences and assessment of the risk to individuals.
Immediate action taken	Action taken to contain the breach and minimise any harm.
Reporting decision/action	Whether the ICO and/or affected individuals were notified; reasons if not; dates/reference if reported. Record whether: • the Chair/Vice-Chair was informed and • whether the breach required reporting to Full Council • whether an Extraordinary Council Meeting was required before the next OCM.
Outcome and prevention	Remedial action taken and any measures introduced to prevent recurrence.