Halton Holegate with Halton Fenside Parish Council

Data Breach Policy

March 2026

Contents

1. Definition

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

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

2. 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.

3. Halton Holegate with Halton Fenside Parish Council's duty to report a breach

If the personal data breach is likely to result in a risk to the rights and freedoms of individuals, the breach must be reported to the Information Commissioner's Office (ICO) without undue delay and, where feasible, not later than 72 hours after becoming aware of it. If the breach is likely to result in a high risk to the rights and freedoms of individuals, those individuals must also be informed without undue delay.

The Clerk/RFO (or other nominated officer) must inform the Council's Data Protection Officer (DPO) immediately on becoming aware of a suspected or actual breach, so that the DPO can assess the incident and, where required, make the ICO notification within the 72-hour timeframe.

When notifying the ICO of a breach, Halton Holegate with Halton Fenside Parish Council must:

i. 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
ii. Communicate the name and contact details of the DPO
iii. Describe the likely consequences of the breach
iv. Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse effects.
v. When notifying the individual affected by the breach, Halton Holegate with Halton Fenside Parish Council must provide the individual with (ii)-(iv) above.

Halton Holegate with Halton Fenside Parish Council will 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.

4. Data processors duty to inform Halton Holegate with Halton Fenside Parish Council

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

5. 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.

6. 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/

7. Procedure and Response

Identify and report immediately

Any Councillor, member of staff, or contractor who becomes aware of a suspected or actual personal data breach must report it to the Clerk/RFO immediately. The Clerk/RFO (or other nominated officer) must inform the Council's Data Protection Officer (DPO) immediately.

Contain and recover

Take prompt steps to limit the impact of the breach, for example: recall an email; contact the unintended recipient and request deletion/return; disable compromised accounts; reset passwords; retrieve paper files; secure premises; isolate affected equipment/systems (where relevant).

Assess what happened

With the DPO's support, establish (as far as possible): what personal data is involved; how many individuals are affected; whether special category data is involved; the cause of the breach; whether the data was protected (e.g., encryption); and whether the breach is ongoing.

Assess risk to individuals

The DPO will assess the likelihood and severity of any risk to individuals' rights and freedoms, considering potential harms (e.g., identity theft, financial loss, distress, loss of confidentiality) and any mitigating factors already in place.

Decide whether notification is required
ICO notification: where the breach is likely to result in a risk to individuals' rights and freedoms, the DPO will notify the ICO without undue delay and, where feasible, within 72 hours of the Council becoming aware of the breach.

Individual notification: where the breach is likely to result in a high risk to individuals' rights and freedoms, the Council will inform affected individuals without undue delay (unless an exception applies under data protection legislation).

Notify the ICO (where required)
The notification will include: (i) the nature of the breach, including categories and approximate number of individuals and records concerned; (ii) the DPO's contact details; (iii) likely consequences; and (iv) measures taken or proposed to address the breach and mitigate adverse effects. If notification is not made within 72 hours, the reasons for delay must be recorded and provided to the ICO.

Communicate with affected individuals (where required)
Communications must be clear and in plain language and include, as appropriate, the nature of the breach, likely consequences, steps taken, and practical advice on how individuals can protect themselves. Where direct notification would involve disproportionate effort, alternative communication may be used in line with DPO advice.

Record the breach
The Clerk/RFO will ensure the breach is recorded in the Council's breach log whether or not it is reportable to the ICO or individuals. The record should include the facts relating to the breach, its effects, and remedial action taken.

Liaise with data processors and third parties
Where a supplier/processor is involved (e.g., payroll provider, website host, cloud service), the Clerk/RFO and DPO will obtain timely information needed for assessment and (if required) ICO/individual notification. Processors must notify the Council without undue delay when they become aware of a breach.

Review and improve
After containment and any necessary notifications, the Council will review root cause, lessons learned, and required improvements (e.g., training, process changes, technical controls, supplier arrangements) to reduce the risk of recurrence.

8. Policy Review

This policy will be review bi-annually.