

Wymeswold Parish Council Data Breach Policy

Definition:

A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. Such examples include:

- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a data controller or data 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.

Notifying the Information Commissioners Office (ICO):

Guidance states that organisations should notify the Information Commissioners Office of a breach where it is likely to result in a risk to the rights and freedoms of individuals or if it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Data Breaches will be recorded using the ICO's online system: <https://ico.org.uk/for-organisations/report-a-breach/> and the following information should be provided:

- The potential scope and cause of the breach.
- Mitigation actions the Council plans to take.
- Details of how the Council plans to address the problem.

Notifying the Individual concerned and Timescales:

If the data breach is likely to result in a risk to the rights and freedoms of the individual (such as through identity theft), the breach must be reported to the individual and the ICO without unnecessary delay and, where feasible, not later than 72 hours after having become aware of the breach. The Data Protection Officer (DPO) must be informed immediately so they are able to report the breach to the ICO in the 72 hour timeframe. In line with the accountability requirements, all data breaches must be recorded by the Council along with details of actions taken. This record will help to identify system failures and should be used to improve the security of personal data.

Notifying the Council:

If anyone (including a third party such as a payroll provider) suspects that a data breach has occurred, they should immediately contact Wymeswold Parish Council with the details. The Council will then contact the ICO with this information.

The Data Protection Officer

Wymeswold Parish Council

Sports Pavilion

Burton Lane,

Wymeswold Parish Council Data Breach Policy

Wymeswold,
LE12 6UN.

Records:

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 following information will be recorded having already been sent to the ICO:

- A description of 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,
- The name and contact details of the DPO,
- A description of the likely consequences of the breach
- A description of the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse effects.

The 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, in all instances, the ICO must still be informed even if the above measures are in place.

Wymeswold Parish Council Data Breach Policy was approved at the Wymeswold Parish Council meeting on Monday 2nd June 2025.
Next Policy Review date June 2028.