

# Data Breach Policy

The 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

This policy applies to all councillors, employees, volunteers, and any third party handling personal data on behalf of Weston-in-Gordano Parish Council (the Parish Council).

Typical categories of personal data handled by the Parish Council include planning-related correspondence, resident enquiries or complaints, volunteer records, and employment-related information.

Weston-In-Gordano Parish Council takes the security of personal data seriously. Computers are password-protected and hard-copy files are kept securely. Councillors and staff using personal devices for Council work must ensure these devices are password-protected and that any personal data is deleted securely once no longer required.

## 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 Parish Council's duty to report a breach

If the data breach is likely to result in a high 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 Clerk and Chairman must be informed immediately so that if they need to, they are able to report the breach to the ICO in the 72 hour timeframe.

If the ICO is not informed within 72 hours, the Parish Council must give reasons for the delay when they report [a reportable] breach. When notifying the ICO of a breach, the 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. Describe the likely consequences of the breach
- iii. Describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse effects.

When notifying the individual affected by the breach, the Parish Council must provide the individual with (ii)-(iii) above.

The 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.

#### Third Party Data processors' duty to inform the Parish Council

If a data processor (e.g. payroll provider) becomes aware that they have experienced a personal data breach, it must notify the Parish Council without undue delay. It is then the Parish Council's (as Data Controller) responsibility to inform the ICO, it is not the data processors responsibility to notify the ICO.

#### Records of data breaches

All data breaches must be recorded whether or not they are reportable to the ICO or individuals. The Clerk is responsible for maintaining the Council's breach log and for coordinating any required notifications to the ICO. This record will help to identify system failures and should be used as a way to improve the security of personal data.

#### Record of Data Breaches

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

Records of data breaches will be retained for six years in accordance with the Council's Document Retention Policy.

To report a data breach use the ICO online system: <https://ico.org.uk/for-organisations/report-a-breach/>

#### Document Versions

Version number	Purpose/change	Author	Date
0.1	Initial draft	DB	March 2025
0.2	Review and Refine	NH	June 2025
0.3	Approved	LS	Nov 2025