Oswestry Rural Parish Council

DATA BREACH POLICY

The General Data Protection Regulations (GDPR) define 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.

Oswestry Rural Parish Council takes the security of personal data seriously; computers are password protected and hard copy files are stored securely.

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. Accordingly, a breach, depending on the circumstances of the breach, can have a wide range of effects on individuals.

The 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 the Information Commissioner's Office (ICO) without undue delay and, where feasible, not later than 72 hours after having become aware of the breach.
If the ICO is not informed within 72 hours, the Parish Council must give reasons for the delay when reporting the breach.

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

1. 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.
2. Provide details of the Council's main point of contact.
3. Describe the likely consequences of the breach.
4. Describe the measures taken, or proposed, to address the personal data breach, including measures to mitigate its possible adverse effects.

When notifying the individual(s) affected by the breach, the Parish Council must provide the individual(s) with the details outlined in 2 to 4 above.

The Parish Council will not need to communicate with individuals if the following applies:

- It has implemented appropriate technical and organisational measures (e.g. encryption) so that 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.

Data Processors' Duty to Inform the Parish Council

If a data processor becomes aware of a personal data breach, it must notify the Parish Council without undue delay. It is then the Parish Council's responsibility to inform the ICO; it is not the data processor's responsibility to notify the ICO.

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.

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/

Policy adopted 26 June 2018