Washingborough
Parish Council

Data Breach Policy

Adopted
21 Jun 2018

Reviewed
20 Jul 2022

Change History

No	Change Type	Updated by	Change summary	Approved by Council
1	Original		Created	21 Jun 2018
2	Update	Policies WP	Added Front sheet & reviewed	20 Jul 2022
3				

Review Interval = Annual

Data Breach Policy

Contents

Definition of a Data Breach

The Data Protection Act 2018 (aka General Data Protection Regulations (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.

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

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.

Washingborough 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 Information Commissioner's Office (ICO) without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. The Data Protection Officer must be informed immediately so they are able to report the breach to the ICO in the 72 hour timeframe.

If the ICO is not informed within 72 hours, Washingborough Parish Council via the DPO must give reasons for the delay when they report the breach.

When notifying the ICO of a breach, Washingborough 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. Communicate the name and contact details of the DPO,
3. Describe the likely consequences of the breach,
4. 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, Washingborough Parish Council must provide the individual with items 2 to 4 above.

Washingborough 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.

Data processors duty to inform Washingborough Parish Council

If a data processor becomes aware of a personal data breach, it must notify Washingborough Parish Council without undue delay. It is then Washingborough Parish Council's 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 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.

A record of Data Breaches should be kept using the following headings -

- Date Of Breach,
- Type of Breach,
- Number of Individuals affected,
- Date reported to ICO,
- Date reported to Individual(s),
- Actions taken to prevent breach recurring.

Reporting Data Breaches to ICO

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