WALBERSWICK PARISH COUNCIL

Draft Data Breach Policy

Proposed for adoption by WPC November 2020

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

Walberswick Parish Council takes security of personal data seriously. Computers are password protected and hard copy files are kept in locked areas.

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.

Walberswick Parish Council's duty to report a breach

The Parish Clerk and the nominated Data Protection Officer must be informed immediately by any member of the Council becoming aware of a data breach. The Parish Clerk should also notify the Council's Chairman of the breach

If the breach is likely to result in a risk to the rights and freedoms of the individual, the breach must be reported by the Parish Clerk or the nominated Data Protection Officer 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.

Data breaches can be reported to the ICO here:

https://ico.org.uk/for-organisations/report-a-breach/

If the ICO is not informed within 72 hours, Walberswick Parish Council via the Parish Clerk or the nominated Data Protection Officer must give reasons for the delay when they report the breach.

When notifying the ICO of a breach the Walberswick 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 nominated Data Protection Officer
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.

When notifying the individual(s) affected by the breach, Walberswick Parish Council must provide the individual(s) with (ii) – (iv) above.

Walberswick Parish Council would not need to communicate with an individual(s) if the following applies:

- It has implemented appropriate technical and organisational measures (e.g. 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 of rights and freedoms of individuals is no longer likely to materialise, or,
- It would involve a disproportionate effort.

Data processors duty to inform Walberswick Parish Council

If a data processor who is processing personal data on behalf of the Walberswick Parish Council (e.g. a payroll provider) becomes aware of a personal data breach, it must notify the Council, via the Parish Clerk or the nominated Data Protection Officer, without undue delay. It is then Walberswick 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 the data subjects involved. This record will help identify system failures and should be used as a way to improve the security of personal data.

The Parish Clerk will maintain a breach register setting out:

I. Date of breach
II. Type of breach
III. Numbers of individuals affected
IV. Date reported to ICO/Individual
V. Actions taken to prevent breach recurring