Sancreed Parish Council

Data Breach Policy

Background

A personal data breach is defined 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" (GDPR).

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.

This policy describes the action that will be taken by the Parish Council in the event of a data breach.

The Duty To Report A Breach

If a data breach is likely to result in a risk to the rights and freedoms of the individual, the Council must report it to the individual and Information Commissioner's Office (ICO) without delay and, where feasible, not later than 72 hours after been made aware of it. If the 72 hour target is missed, the Council must give reasons for the delay when reporting the breach.

Reporting A Breach To The ICO

A breach will be reported to the ICO by the Clerk (as the Council's Data Protection Officer) using https://ico.org.uk/for-organisations/report-a-breach.

When notifying the ICO and the individual of a breach, the Clerk must

a) 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
b) give the name and contact details of the DPO
c) describe the likely consequences of the breach
d) describe the measures taken or proposed to be taken to address the personal data breach including, measures to mitigate its possible adverse effects.

Reporting A Breach To An Affected Individual

A breach will be reported to an affected individual by the Clerk (as the Council's Data Protection Officer).

When notifying the individual affected by the breach, the Clerk must provide the individual with b-d above.

The Parish Council would not need to communicate with an individual if the following applies:

a) 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
b) It has taken subsequent measures to ensure that the high risk to rights and freedoms of individuals is no longer likely to materialise, or

c) 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 (e.g. a payroll provider) 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 of the breach - not that of the data processor.

Records Of Data Breaches

All data breaches will be recorded whether or not they are reported to individuals. This will help to identify system failures and to improve the security of personal data.

For each data breach, the following will be recorded:

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