CORRINGHAM PARISH COUNCIL

Data Breach Policy

ADOPTED February 2022

Reviewed May 2026

CORRINGHAM PARISH COUNCIL

Scope

This policy defines the roles and responsibilities of Corringham Parish Council regarding a suspected or real data breach. electronic communications and use of the internet. Councillors and Proper Officers alike are responsible for ensuring compliance with this and related policies.

A separate policy on **Electronic Communication, Press and Social Media Policy** is available and should be considered in conjunction with this policy.

Introduction

The General Data Protection Regulations 2018 (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". Corringham Parish Council takes the security of personal data seriously and takes the necessary steps to ensure that data is protected.

Examples of a data breach 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

1. 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.

2. Corringham Parish Council's Duty to Report a Breach

Should Corringham Parish Council be made aware of a personal data breach it shall take the necessary steps to consider whether it poses a risk to people via the Information Commissioner's Office (ICO) Self assessment for data breaches tool https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/ . When the Parish Council has made this assessment, if it's likely there will be a risk then it will notify the ICO; if it's unlikely there will be a risk, the Parish Council may not be required to report it.

Corringham Parish Council do not need to report every breach to the ICO, but 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 ICO without undue delay and, where feasible, not later than 72 hours after having become aware of the breach.

A data breach may be reported to the ICO via their online system:
https://ico.org.uk/for-organisations/report-a-breach/

The Data Protection Officer must be informed within 48 hours so they are able to report the breach to the ICO in the 72 hour time frame.

If the ICO is not informed within 72 hours, Corringham Parish Council, via the Data Protection Officer (DPO) must give reasons for the delay when they report the breach.

When notifying the ICO of a breach, Corringham 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 DPO

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 affects.

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

Corringham 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.

3. Duty of Data Processors

If a data processor (i.e., payroll provider) becomes aware of a personal data breach, it must notify Corringham 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.

4. 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.

Records should include as a minimum details of:

- Date of breach
- Nature of breach
- Number of individuals affected
- Date reported to ICO/The Individuals
- Actions to Prevent Breach Occurring

Related Policies

Electronic Communication, Press and Social Media Policy