PAPPLEWICK PARISH COUNCIL

GDPR Data Breach Policy

This policy was adopted at a Parish Council meeting on 14th January 2026

Purpose

The purpose of this policy is to:

- Define what constitutes a data breach.
- Establish the steps to follow in the event of a data breach.
- Ensure compliance with GDPR regulations.
- Minimize the impact of data breaches on individuals and the Parish Council.

Scope

This policy applies to all employees, contractors, Parish Councillors and third parties handling personal data within and on behalf of the Parish Council.

Definition of a Data Breach

A data breach is defined as a security incident that results in the accidental or unlawful, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed by the organization.

Types of Data Breaches

Data breaches can be categorized into three main types:

- Confidentiality breach: Unauthorized access or disclosure of personal data.
- Integrity breach: Unauthorized alteration or destruction of personal data.
- Availability breach: Loss or destruction of personal data, resulting in data being unavailable.

Reporting a Data Breach

Employees, contractors, parish councillors and third-party service providers must report any suspected or confirmed data breaches immediately to the Parish Council. Once reported, an investigation should take place into the reasons for and potential consequences of the suspected data breach.

The results of the investigation should include:

- The nature of the breach.
- The categories and approximate number of data subjects affected.
- The categories and approximate number of personal data records affected.
- The consequences of the breach.
- Any measures taken or proposed to address the breach.

Data Breach Response

The Parish Council is responsible for reviewing the investigation into the breach, and concluding on the appropriate course of action.

Data Breach Response Procedure

PPC will follow these steps in the event of a data breach:

- Identify and contain the breach to prevent further unauthorized access or disclosure.
- Review the results of the investigation and conclude on whether the breach is reportable to the Office of the Information Commissioner. Breaches of personal information should be reportable to the regulator unless they are “unlikely to result in a high risk to the rights and freedoms of natural persons”.
- Notify the Information Commissioner within 72 hours of becoming aware of the breach, if required by GDPR.
- Notify affected data subjects without undue delay, if the breach is likely to result in a substantial risk to their rights and freedoms.
- Document all details of the breach and the response actions taken.
- Conduct a post-incident review to identify lessons learned and improve security measures.

Notification to Data Subjects

If the data breach is likely to result in a substantial risk to the rights and freedoms of affected data subjects, the Parish Council will notify the data subjects without undue delay. The notification will include:

- The nature of the breach.
- The name and contact details of the Parish Council.
- The consequences of the breach.
- Any measures taken or proposed to address the breach and mitigate its potential adverse effects.

Record Keeping

The Parish Council will maintain a record of all data breaches, regardless of whether they are notifiable to the supervisory authority. The records will include:

- The nature of the breach.
- The categories and approximate number of data subjects affected.
- The categories and approximate number of personal data records affected.
- The consequences of the breach.
- Any measures taken or proposed to address the breach

Review and Updates

This policy will be reviewed (where necessary) and updated as required to reflect changes in legal, regulatory, or operational requirements. The Council is responsible for ensuring that the policy remains current and compliant with GDPR principles.