



PERSONAL DATA BREACH POLICY

Review Date: 15th December 2025

Introduction

This Personal Data Breach Policy sets out the procedures Carharrack Parish Council ("the Council") has in place to deal with any breach affecting the confidentiality, integrity, or availability of personal data processed by the Council.

Carharrack Parish Council
c/o 8 Albion Row, Carharrack, Redruth, TR16 5QW
("the Organisation", "we", "our")

The Council is a **Data Controller** for personal data in accordance with all applicable data protection and privacy laws, including (but not limited to):

- The UK GDPR (retained from EU Regulation 2016/679)
- The Data Protection Act 2018
- The Privacy and Electronic Communications Regulations 2003 (as amended)
- Any subsequent or successor legislation (collectively, the Data Protection Legislation).

This policy is binding on all employees, councillors, contractors, and volunteers ("Users") who access or process personal data on behalf of Carharrack Parish Council.

The policy applies to all filing systems, whether electronic, paper-based, centralised, decentralised, or dispersed.

Definitions

1.1 Personal Data

Personal data means any information relating to an identified or identifiable individual ("data subject"). An individual is identifiable if they can be identified directly or indirectly by reference to an identifier such as:

- Name
- Identification number
- Location data
- Online identifier
- Factors relating to physical, genetic, mental, economic, cultural or social identity

1.2 Nature of Personal Data

Personal data may include information about an individual's activities or circumstances.

1.3 Personal Data Breach

A personal data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This includes incidents caused by both accidental and deliberate actions.

1.4 Examples of Personal Data Breaches

Personal data breaches include, but are not limited to:

- Access by an unauthorised third party.
- Deliberate or accidental action/inaction by a data controller or processor
- Sending personal data to an incorrect recipient
- Loss or theft of devices containing personal data
- Loss or theft of paper files containing personal data.
- Alteration of personal data without permission.
- Loss of availability of personal data (e.g., system outage)

1.5 Broad Definition

A personal data breach is any incident affecting confidentiality, integrity or availability of personal data.

1.6 Significant Negative Effect

A breach occurs where personal data is lost, disclosed, corrupted, or accessed without proper authorisation, or where data becomes unavailable and the unavailability has a significant negative effect on individuals.

Responsibility for Managing Personal Data Breaches

2.1 Oversight

Council Officers (the Clerk and/or appointed Data Protection Lead) are responsible for ongoing monitoring and compliance with this policy and all relevant Data Protection Legislation.

2.2 Adherence

Users must not deviate from this policy without written authorisation from Council Officers.

Time Limits

3.1 Reporting to the ICO

Not all personal data breaches must be reported to the Information Commissioner's Office ("ICO").

However, breaches that pose a risk to individuals' rights and freedoms must be reported within 72 hours of the Council becoming aware of the breach.

3.2 Non-working Days

The 72-hour deadline applies regardless of weekends or bank holidays.

3.3 Internal Notification

Users must notify Council Officers in writing within 1 hour of becoming aware of a suspected or actual breach.

Investigation

4.1 Initial Review

Council Officers will investigate suspected breaches to determine their nature, cause and impact.

4.2 Preventative Review

The investigation will consider whether the breach could occur again and how to prevent recurrence.

4.3 Human Error

Where human error is the cause, the investigation will review:

- Adequacy of user training (induction and refresher)
- Adequacy of supervision and support for users
- Whether policies and procedures require updating

4.4 Systemic Issues

Where the breach results from system failings, the investigation will consider:

- Whether access permissions are appropriate
- Whether a broader system audit is required
- Whether current technical and organisational measures remain adequate
- Whether additional measures need to be implemented

Notifying the ICO

5.1 Determining Risk

The ICO must be notified where a breach is likely to result in a risk to individuals' rights and freedoms.

- Where such risk exists, the Council must notify the ICO within 72 hours.
- Where such risk is unlikely, the Council is not required to report but may choose to submit a voluntary report.

5.2 Documentation of Decision

If a breach occurs and the Council decides not to report it to the ICO, the decision and rationale must be recorded in the Carharrack Parish Council Breach Register.

5.3 Reporting

If a breach is reported to the ICO, this must also be documented in the Breach Register.

Notifying Data Subjects

6.1 When Notification is Required

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Council must notify those affected without undue delay.

The notification must include:

- A description, in clear and plain language, of the nature of the breach
- Includes the name and contact details of Council Officers for further information
- The likely consequences of the breach
- The measures taken or proposed to address the breach, including mitigation steps

6.2 Advice and Support

Where possible, Council Officers should give clear, specific advice to affected individuals on actions they can take to protect themselves, and what assistance the Council will provide.

This advice may include, but is not limited to:

- Resetting passwords
- Using strong, unique passwords
- Being alert to phishing, identity theft or suspicious contact
- Monitoring bank or account activity if financial data is involved
- Contacting relevant service providers to secure accounts

Users' Role in Personal Data Breaches

7.1. Users must notify Council Officers in writing immediately, and in any event within 1 hour, of any actual or suspected personal data breach.

7.2. Users must not attempt to contain, investigate, or rectify a breach without prior instruction or authorisation from Council Officers.

7.3. Users must provide full, accurate and timely assistance to Council Officers during any investigation.

7.4. Obstruction or failure to cooperate with an investigation will be addressed through the appropriate disciplinary or conduct procedures.

Updates to This Policy

8.1. This policy shall be reviewed **annually** by Council Officers or sooner if changes in legislation, ICO guidance, or Council processes require it.


8.2 This policy shall also be reviewed if Carharrack Parish Council makes changes to the

organisations **Privacy Notice** or if there are changes to how the Council processes personal data, or if data protection legislation changes.

8.3. This policy was last updated on 8th December 2025 and reviewed at Council Meeting 15th December 2025 as detailed in meeting point 16.

Implementation

9.1. This policy takes effect from 15th December 2025 and is not retroactive

Name	Position	Signature	Date
Cllr Bettina Holland	Chairperson		15.12.2025