Data Breach Policy – March 2026

BUCKLESHAM PARISH COUNCIL

Ruth Johnson
CLERK, BUCKLESHAM PARISH COUNCIL

Introduction

Bucklesham Parish Council is committed to protecting the personal data it processes and to complying with the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This Policy sets out how the Council will identify, manage, report and learn from personal data breaches in a consistent, lawful and proportionate manner.

This Policy applies to all Councillors, Officers, contractors, volunteers and others who process personal data on behalf of the Council.

All actual, suspected or potential data breaches, including near misses, must be reported immediately to the Parish Council Clerk.

What is a Personal Data Breach?

A personal data breach is a breach of security leading to the accidental or unlawful:

- destruction;
- loss;
- alteration;
- unauthorised disclosure of; or
- access to personal data.

A breach may involve confidentiality, integrity or availability of personal data and may result in harm to individuals, disruption to Council services, reputational damage, financial loss or regulatory enforcement.

Examples (non-exhaustive) include:

- personal data sent to the wrong recipient;
- loss or theft of devices, paper files or storage media containing personal data;
- unauthorised access to systems or records;
- cyber incidents such as malware or phishing attacks;
- insecure disposal of personal data;
- physical security failures resulting in unauthorised access to records.

Near misses, where a breach was narrowly avoided, must also be reported so that learning and mitigation can take place.

Roles and Responsibilities

Parish Council Clerk

The Parish Council Clerk is responsible for overseeing the management of data breaches on behalf of the Council, including:

- assessing the breach and associated risks;
- determining whether notification to the Information Commissioner's Office (ICO) and/or affected individuals is required;
- ensuring incidents are recorded, investigated and resolved; and
- ensuring lessons learned are acted upon.

Councillors, Officers, Contractors and Volunteers

All individuals processing personal data on behalf of the Council are responsible for:

- identifying and reporting suspected or actual data breaches immediately;
- cooperating with any investigation; and
- taking steps to contain and mitigate breaches where safe to do so.

Reporting a Data Breach

All data breaches or suspected breaches must be reported as soon as they are discovered to the Parish Council Clerk.

Where an incident occurs outside normal working hours, it must be reported at the earliest practicable opportunity by email or telephone.

Where there is doubt as to whether an incident constitutes a breach, it must be treated as a breach and reported.

Incident Response and Management

The Council will follow a structured incident response process:

1. **Identification and Assessment**

   Confirm whether a personal data breach has occurred, assess the nature and scope of the incident, and identify the categories and volume of personal data involved.

2. **Containment and Mitigation**

   Take immediate steps to limit the impact of the breach, including securing systems, recovering data where possible, and preventing further unauthorised access or loss.

3. **Risk Assessment**

   Assess the likelihood and severity of the risk to the rights and freedoms of affected individuals, taking account of:

   - the type of data involved;
   - the sensitivity of the data;
   - the number of individuals affected; and
   - the potential consequences of misuse.

4. **Notification Decisions**

   The Parish Council Clerk will determine, based on risk assessment:

   - whether the breach must be reported to the ICO (within 72 hours of becoming aware of the breach, where required); and
   - whether affected individuals must be informed without undue delay.

5. **Recovery and Remediation**

   Restore systems and processes, provide appropriate support to affected individuals where necessary, and implement measures to prevent recurrence.

6. **Review and Learning**

   All breaches and near misses will be reviewed to identify lessons learned and any required changes to policies, procedures, training or technical controls.

Recording and Documentation

All personal data breaches and near misses will be recorded in a data breach log, regardless of whether they are reported to the ICO.

Records will include:

• the facts relating to the breach;

• its effects; and

• remedial action taken.

Disciplinary and Compliance Matters

Failure to comply with this Policy may result in disciplinary action where breaches arise from deliberate, reckless or repeated non-compliance with Council policies or procedures.

Nothing in this Policy is intended to deter prompt reporting. Early reporting of mistakes or near misses is encouraged and supported.

Review and Monitoring

This Policy will be monitored for effectiveness and reviewed biennially, or earlier where required due to legislative change, ICO guidance or operational learning.

Adopted by the Parish Council at a meeting on: 11th March 2026

Signed:

Ruth Johnson

Ruth Johnson
Clerk

Clive Lenton

Clive Lenton
Chair

Version Control

Date	Details	Next Review
11th March 2026	First Publication	September 2027
September 2027	Annual Review	