Buckhorn Weston and Kington Magna Parish Council

Durfold Cottage, Church Hill, Buckhorn Weston, Dorset, SP8 5HS, Tel: 07787 784009
Email:clerk@buckhornwestonkingtonmagna-pc.gov.uk
www.buckhornwestonkingtonmagna-pc.gov.uk

DATA SECURITY POLICY

1. Purpose of the Policy

The purpose of this policy is to protect the confidentiality, integrity, and availability of Buckhorn Weston & Kington Magna Parish Council's information and maintain public trust by ensuring the secure handling of personal and sensitive data. The policy is also to ensure compliance with the UK GDPR, Data Protection Act 2018, and other statutory duties and minimise the risk of data breaches and operational disruption.

2. Roles & Responsibilities

The Data Controller with ultimate responsibility is Buckhorn Weston & Kington Magna Parish Council. The Clerk / Proper Officer is the Data Protection Lead who manages compliance, breach response and training. Councillors, staff and volunteers must follow all data protection and IT-security procedures.

3. Data Protection Principles (UK GDPR)

Personal data must be:

- Processed lawfully, fairly, and transparently.
- Collected for specific, legitimate purposes.
- Adequate, relevant, and limited to what is necessary.
- Accurate and kept up to date.
- Stored securely and retained only as long as necessary.

IT & Information Security Controls

4.1 Access & Authentication

Strong passwords are essential with password sharing not permissible. Accounts must be for individuals only with no shared logins. The additional security of multi-factor authentication should be applied where possible.

4.2 Email & Domain Use

All official business must be carried out on council-owned domain emails (e.g. clerk@buckhornwestonkingtonmagna-pc.gov.uk). Personal email accounts (Gmail, Hotmail, etc.) are not to be used for council business.

4.3 Device & Software Security

Only approved software is permitted with regular updates, anti-virus and anti-malware protection required. Laptops, USBs, and backups should be encrypted. The use of Office 365, or an equivalent, should be securely configured.

4.4 Remote Working
Secure connections should be used such as VPN or encrypted services. Council data must not be stored on personal devices unless authorised and protected.

4.5 Removable Media
USB sticks should be avoided, unless encrypted, and a register of removable media should be maintained if used.

5. Data Handling & Storage
Paper and electronic records are stored securely with access limited only to those with a legitimate need. Defined retention periods and secure disposal procedures are in place.

6. Website & Publication Requirements
The Parish Council website complies with WCAG 2.2 AA accessibility standards where all statutory documents under FOIA 2000 and the Transparency Code are published.

7. Training & Awareness
Training is available for councillors and staff on:

- UK GDPR & Data Protection Act
- FOI obligations
- Cybersecurity best practice
- Council IT policies

8. Data Breach Reporting & Incident Management
A breach includes unauthorised access, loss, disclosure, or destruction of personal data. Examples are:

- Sending data to the wrong recipient
- Lost or stolen devices
- Ransomware attacks

Breach Procedure

1. Immediate reporting to the Clerk (Data Breach Manager).
2. Containment: isolate systems, reset passwords, secure records.
3. Assessment: determine risk to individuals.
4. Notification:
    - ICO within 72 hours if risk is likely.
    - Affected individuals if high risk.
5. Record breach in the Breach Register.

9. Record-Keeping & Audit
A log is maintained which includes data audits, policy approvals, training records and security incidents.

This policy will be reviewed annually or after major legislative/technical changes.