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 Breach Policy

1. Purpose

This policy sets out how Buckhorn Weston & Kington Magna Parish Council will identify, manage, and report personal data breaches in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Its aim is to protect individuals' rights and ensure the council responds quickly and effectively to any breach.

2. Scope

This policy applies to:

- All councillors
- The Clerk and Responsible Financial Officer
- Any volunteers or contractors handling personal data on behalf of the council

It covers all personal data processed by the council, whether held electronically, on paper, or in any other format.

3. What Is a Data Breach?

A personal data breach is any incident that results in:

- Unauthorised access to personal data
- Accidental or unlawful destruction, loss, alteration, or disclosure
- Personal data becoming unavailable (e.g., ransomware, system failure)

Examples include:

- Sending personal information to the wrong recipient
- Losing an unencrypted USB stick
- Email accounts being hacked
- Accidental deletion of records without backup
- Paper records left unsecured

4. Identifying and Reporting a Breach

Anyone who becomes aware of a possible breach **must report it immediately** to the Clerk (or Chair if the Clerk is unavailable).

Reports should include:

- What happened
- When it happened
- What data was involved
- Who is affected
- Any immediate actions taken

No one should attempt to hide or ignore a breach.

5. Initial Assessment
The Clerk (or Chair) will:

- Record the incident in the Data Breach Log
- Assess the nature and severity of the breach
- Determine whether the breach is likely to pose a risk to individuals' rights and freedoms

If needed, the council may seek advice from:

- The Data Protection Officer (if appointed)
- The Information Commissioner's Office (ICO) helpline

6. Recording the Breach
All breaches—whether reportable or not—must be logged.
The log will include:

- Date and time of breach
- Description of the incident
- Categories of data affected
- Number of individuals affected
- Actions taken
- Whether the ICO was notified
- Lessons learned

7. Notifying the ICO
The council **must notify the ICO within 72 hours** if the breach is likely to result in a risk to individuals (e.g., identity theft, financial loss, distress).
The notification will include:

- Nature of the breach
- Categories and approximate number of individuals affected
- Likely consequences
- Measures taken or proposed

If the council decides **not** to report the breach, the reasoning must be documented.

8. Notifying Individuals
If the breach is likely to result in a **high risk** to individuals, the Parish Council must inform affected people **as soon as possible**, using clear and plain language.
The notification will explain:

- What happened
- What data was involved
- What the council has done
- What individuals can do to protect themselves
- Contact details for further information

9. Containment and Recovery
The council will take immediate steps to:

- Stop the breach
- Secure systems or records
- Recover lost data where possible
- Prevent further unauthorised access

This may include changing passwords, restoring backups, or contacting third-party service providers.

10. Review and Prevention

After each breach, the council will review:

- What went wrong
- Whether policies or procedures need updating
- Whether staff or councillors need additional training
- Whether technical safeguards should be improved

Lessons learned will be documented in the Data Breach Log.

11. Policy Review

This policy will be reviewed **annually** or sooner if:

- Legislation changes
- The council's data processing activities change
- A significant breach occurs