Benwick Parish Council

Information Technology & Acceptable Use Policy

Adopted at meeting on 5 January 2026 (minute ref: 157/25-26)

1. Introduction

This policy sets out the Council's expectations for the secure and appropriate use of information technology (IT) and electronic communications. It ensures the Council meets its legal duties under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Freedom of Information Act 2000, and the governance requirements of the Annual Governance and Accountability Return (AGAR), particularly Assertion 10 on risk management.

Benwick Parish Council is a small authority with limited resources and one employee. Councillors and the Clerk routinely use personal devices to carry out council business. This policy therefore takes a proportionate, risk-based approach suitable for a parish council with a small precept.

2. Scope

This policy applies to:
- The Clerk
- All elected and co-opted councillors
- Any authorised volunteers or contractors acting on behalf of the Council

It covers the use of:
- Council email accounts
- Personal devices used for council business
- Internet use
- Electronic communication
- Social media where it relates to council activity

3. Roles and Responsibilities

<u>The Clerk</u>
- Manages Council email accounts and acts as the primary point of contact for IT issues.
- Ensures security incidents or data breaches are reported and handled in line with the Data Protection Policy.
- Maintains an inventory of any Council-owned IT assets (currently limited to the Clerk's laptop).

<u>Councillors</u>
- Use their council-issued email account for council business.
- Keep personal devices secure when used for Council work.
- Report any lost or compromised devices immediately.

Website and Email Providers
- The Council's .gov.uk email is hosted by Zoho, which provides its own security and authentication systems.
- The Parish Online website provider is responsible for the security of the website platform as far as the contract extends.

4. Council-Issued Equipment

The Council currently does not issue devices to councillors due to budget constraints and the small size of the authority. Councillors may therefore use personal devices for council business, provided they follow the security measures set out in Section 5.

The Clerk uses a council-owned laptop, which must not be used for personal activities.

5. Use of Personal Devices (Bring Your Own Device)

Where councillors or the Clerk use personal devices (mobile phones, tablets, or computers) for council business, the following reasonable security measures must be followed:

<u>Required</u>
- A screen lock/PIN/password or biometrics (e.g facial recognition) must be enabled.
- Devices must be kept up to date (system updates and security patches).
- Devices should not be shared while logged into council accounts.
- The council email account must be accessed only through the official .gov.uk Zoho system.
- Council documents should be kept within email or the council's online storage and not permanently downloaded when avoidable.
- Lost, stolen, or compromised devices must be reported to the Clerk immediately.

<u>Not required</u>
The Council does not require:
- Remote wiping of personal devices
- Installation of monitoring software
- Device encryption beyond what is built into modern devices
- Clerk access to personal devices

6. Email Use

- All council business must be conducted using the benwickparishcouncil.gov.uk email addresses.
- Personal email accounts must not be used for council business.
- Passwords must follow National Cyber Security Centre guidance (three random words) and multi-factor authentication (MFA) must be enabled where possible.
- Emails containing personal data should be handled carefully and only shared where necessary and lawful.

7. Data Handling and Storage

- Council information should be stored within the Zoho email system or other approved council systems.
- Documents containing personal data should not be saved permanently on personal devices unless unavoidable and must be deleted after use.
- Printed documents must be kept secure and shredded once no longer needed.
- Memory sticks or external drives should not be used unless agreed with the Clerk.

8. Remote Working

When working away from home or the office:
- Be aware of who may be able to see your screen (e.g., on public transport).
- Avoid accessing council email on unsecured public computers.
- If you must print documents, store them securely and dispose of them safely.

9. Internet Use

- Users must not access illegal or inappropriate content using council email accounts or when acting on behalf of the council.
- Users must not download or share copyrighted materials unlawfully.
- Users must be cautious when opening links or attachments from unknown sources.

10. Social Media Use

General Principles:
- Councillors and the Clerk must follow the Members' Code of Conduct.
- Posts should be respectful, factual and not bring the council into disrepute.
- Do not publish confidential information or personal data.
- Councillors' personal social media accounts should clearly state that views are their own if discussing local matters.
- The Clerk is the point of contact for any media enquiries.

11. Acceptable Use

All users must:
- Use IT systems in a lawful, respectful and responsible manner.
- Not access or distribute material that is discriminatory, abusive, threatening, obscene, or illegal.
- Not use council email or systems to harass, bully, or intimidate any person.
- Not expose the Council to reputational damage.
- Not represent personal views as those of the Council.

12. Monitoring

The Council does not routinely monitor the content of councillor or staff communications.

However, monitoring may occur only if:
- required to investigate a data breach or security incident
- required by law enforcement
- necessary to resolve a technical problem
- needed to comply with legal obligations

13. Reporting Incidents

All users must promptly report to the Clerk:
- lost or stolen devices
- suspected hacking or unauthorised access
- mis-sent emails containing personal data
- any suspected data breach

The Clerk will follow the Data Breach Procedure and notify the ICO where legally required.

14. Review

This policy will be reviewed at least every two years, or sooner if legislation, systems, or circumstances change.