Birdlip Parish Council

Birdlip Parish Council Bring Your Own Device (BYOD) Policy

1. Purpose

This Bring Your Own Device (BYOD) Policy sets out the conditions under which councillors, employees, and contractors of Birdlip Parish Council may use personally owned devices to access, process, or store Council information. The policy ensures that the confidentiality, integrity, and availability of information are protected and that the Council meets its obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018.

2. Scope

This policy applies to all personally owned devices used for Council business, including but not limited to:

- Mobile phones (smartphones)
- Tablets
- Laptops and home computers

It applies to all users who access Council systems, email, files, or personal data using a personal device.

3. Policy Statement

Birdlip Parish Council permits BYOD use where it is practical and proportionate, provided that appropriate security and governance controls are in place.

The Council remains the Data Controller for all personal data processed on personal devices for Council purposes.

4. Roles and Responsibilities

4.1 Birdlip Parish Council

- Ensures appropriate policies, procedures, and guidance are in place for BYOD use.
- Reviews this policy annually or following a security incident.

4.2 Clerk to the Council (or Data Protection Lead)

- Acts as the responsible officer for BYOD governance.
- Ensures that risks associated with BYOD are identified and managed.
- Maintains oversight of compliance with data protection and information security requirements.
- Acts as the point of contact for data protection incidents involving personal devices.

4.3 Users

- Comply fully with this policy and all related Council policies.
- Take reasonable steps to protect Council information on their personal devices.
- Immediately report loss, theft, or suspected compromise of a device used for Council business.

5. Acceptable Use

Personal devices may only be used for:

- Accessing Council email accounts
- Accessing approved cloud services or document repositories
- Communicating with councillors, officers, or members of the public on Council business

Council data must not be:

- Stored unnecessarily on the device
- Shared with unauthorised individuals
- Used for personal, political, or commercial purposes unrelated to Council business

6. Security Requirements

All personal devices used for Council business must:

- Be protected by a strong password, PIN, or biometric control
- Automatically lock after a short period of inactivity
- Use up-to-date operating systems and security patches
- Have reputable anti-malware software installed where applicable
- Encrypt data where the device supports encryption

Users must not:

- Jailbreak or root devices used for Council business
- Disable security controls required by this policy

7. Storage and Transfer of Data

- Personal data and sensitive Council information should, wherever possible, be accessed remotely and not stored locally on personal devices.
- Any locally stored Council data must be deleted as soon as it is no longer required.
- Council data must only be transferred using Council-approved systems and services.

8. Monitoring and Access

The Council does not routinely monitor personal devices. However, to meet its accountability obligations, the Council may:

- Require confirmation that security controls are in place
- Request the removal of Council data from a personal device
- Withdraw BYOD approval where risks are identified

The Council will not access personal content on a device.

9. Data Breaches and Incident Reporting

Any actual or suspected data breach involving a personal device must be reported immediately to the Clerk to the Council.

This includes:

- Loss or theft of a device
- Unauthorised access to Council data
- Accidental disclosure of personal data

The Council will assess incidents in line with its Data Breach Procedure and, where required, report to the Information Commissioner's Office (ICO).

10. Leaving Role or Withdrawal of BYOD Privilege

When a user:

- Leaves their role with the Council, or
- Is instructed to cease using a personal device for Council business

They must:

- Remove all Council data and accounts from their personal device
- Confirm in writing that Council data has been securely deleted

11. Compliance and Review

Failure to comply with this policy may result in withdrawal of BYOD privileges and, where appropriate, further action in line with Council procedures.

The policy will be reviewed annually and following any significant change in legislation, guidance, or Council operations.

Policy Adopted 17th February 2026

Next Review Date February 2027