

Broadclyst Parish Council

Draft Bring Your Own Device (BYOD) Policy

Version: 1.0

Adopted on: _____

Owner: Clerk (or Chair of Council for matters relating to the Clerk)

Review cycle: Annual or upon material change to legislation/technology

Applies to: Officers and Councillors

1) Purpose

To set clear rules for using personal devices to access Council systems and information, ensuring compliance with UK GDPR/Data Protection Act 2018 and good cyber security practice.

2) Scope & Definitions

- Personal device (BYOD): A smartphone, tablet, laptop or home computer not owned by the Council.
- Council data: Any information created, received, or held in the course of Council business (including emails, documents, Teams chats, recordings and contacts).
- Systems covered: Microsoft 365 services including Outlook/Exchange (email), Teams and OneDrive/SharePoint.

3) General Principles (apply to everyone)

- Council data must be kept within Microsoft 365. Do not store Council documents on local/personal storage or third-party cloud services.
- Multi-Factor Authentication (MFA) is required for all Microsoft 365 access.
- Devices used for Council work must be:
 - Protected by a strong passcode/biometric lock,
 - Encrypted at rest (e.g., FileVault/BitLocker; modern iOS/Android are encrypted by default),
 - Running supported OS versions with current security updates, and not jail-broken or rooted
- Loss/theft, suspected compromise or mis-sent data must be reported to the Clerk/DPO immediately (within 24 hours of the discovery of data loss).

A) Officers (Staff)

A1. Default position

- BYOD is not encouraged. Officers should normally use Council-issued devices.

A2. Exception by approval only

- BYOD may be permitted case-by-case with written approval from the Clerk (or from the Chair of Council where the Clerk is the applicant).
- Approval will specify the systems, duration and conditions. Approval can be withdrawn at any time.

A3. Mandatory controls for approved officer BYOD

- Access limited to Microsoft 365 apps (Outlook, Teams, OneDrive) with MFA.
- No local storage of Council documents or email archives (.pst/.olm).
- Microsoft app protection policies and/or Intune device management may be required (e.g., to enforce PIN, block copy/paste to personal apps, enable selective wipe).
- Backups of Council data to personal devices or services are prohibited.

A4. Acceptable use & support

- Devices remain personal property; the Council may require installation of management or protection profiles that only govern Council data.
- IT support from the Council is limited to accessing Microsoft 365; general consumer support remains the user's responsibility.

B) Councillors

B1. What's allowed

- Councillors may use personal devices to access Teams, email (Office 365/Outlook), and OneDrive for Council business, subject to this policy.

B2. Storage rule (OneDrive-only)

- Store Council documents only in OneDrive/SharePoint.
- Do not store Council files on device local storage, personal email, USB sticks, Dropbox, iCloud Drive, Google Drive or similar.

B3. Devices provided on request

- Where a Councillor does not have a suitable device, the Council will issue a simple tablet configured for Council use only.

B4. Security requirements

- Enable device passcode/biometric, encryption, auto-lock ≤ 5 minutes, and keep OS/apps updated.
- Only use Microsoft apps and MFA
- Where devices are shared with family members the device must be secured using separate logins and accounts.
- Do not share your device unlocked with others when Council data is visible; family/shared use must not expose Council accounts or files.
- Do not forward Council emails to non-Council accounts or use non-Council messaging platforms for Council business.

B5. Data protection & access requests (UK GDPR)

- Emails, Teams messages, and files you hold in Microsoft 365 for Council business may contain personal data and can be subject to Data Subject Access Requests (DSARs), erasure/rectification requests, and disclosure obligations.
- If you receive or are notified of a request, inform the Clerk/DPO immediately and cooperate to locate relevant records. Redaction/anonymisation will be applied as advised by the Clerk/DPO.
- Keep records accurate, minimal and relevant to your role; avoid keeping duplicate or unnecessary copies.

B6. Records management & end of term

- Keep only information strictly relevant to your Councillor role and only for your term of office, in line with Council retention rules.
- On leaving office (or changing role):
- Return any issued device and accessories,
- Delete or transfer to Council officers any personal, sensitive or commercial data related to Council business that is not specifically required for your own duties,
- Allow the Council to perform a selective wipe of Microsoft 365 data from your personal device if app protection/device management is in place.

4) Prohibited activities

- Local or third-party cloud storage of Council documents.
- Sharing Council data via personal messaging or personal email.
- Disabling security controls (MFA, device encryption, app protection).
- Using jail-broken/rooted devices for Council access.
- Installing unlicensed software to process Council data.
- Recording meetings or calls without proper Council authority.

5) Monitoring, Privacy & Access Revocation

- The Council does not monitor personal content on BYOD devices. Controls (e.g., app protection) apply only to Council data/containers.
- The Council may revoke access where policy compliance, cyber risk, or legal obligations require it.

6) Incident Reporting

Report immediately to the Clerk/DPO:

- Lost/stolen device,
- Suspected malware or account compromise,
- Mis-directed email or data disclosure,
- Any request relating to personal data (e.g., DSAR).

7) Compliance & Enforcement

Non-compliance may result in withdrawal of access, device wipe of Council data, and where relevant, action under the Officer HR procedures or Members' Code of Conduct.

8) Review

This policy will be reviewed annually or upon significant change in law, risk or technology.

Appendix 1

Officers (BYOD – approved exceptions only)

- ☐ Written approval in place
- ☐ Microsoft 365 apps + MFA only
- ☐ No local/third-party storage
- ☐ Device encrypted, updated, auto-lock ≤ 5 mins
- ☐ App protection/Intune configured if required
- ☐ Report incidents to Clerk/DPO immediately

Councillors

- ☐ Use Outlook, Teams, OneDrive only
- ☐ Store files only in OneDrive/SharePoint
- ☐ Device passcode/biometric, encryption, updates on
- ☐ MFA enabled
- ☐ No forwarding to personal email or non-Council apps
- ☐ Cooperate promptly with DSARs via Clerk/DPO
- ☐ Report incidents to Clerk/DPO immediately
- ☐ On leaving return/delete/transfer Council data

Appendix 2 – Acknowledgement (to be signed)

I acknowledge receipt of the Broadclyst Parish Council BYOD Policy (v1.0). I understand my responsibilities and agree to comply. I consent to the use of Microsoft security controls (e.g., MFA and app protection) on any personal device I use for Council business.

Name: _____

Role (Officer/Councillor): _____

Signature: _____ Date: ____ / ____ / ____