BECKLEY VILLAGE HALL

Registered charity number 305168

CYBER & DATA SECURITY POLICY

Document Control

- **Approved by Trustees on:** [Date]
- **Next Review Date:** [Date]
- **Policy Owner:** [e.g., Secretary / Chair]

---

1. Purpose & Scope
This policy outlines how Beckley Village Hall protects its digital data, email accounts, financial transactions, and public Wi-Fi infrastructure.

Because the Hall operates without physical on-site computers, this policy applies directly to all trustees, booking volunteers, and committee members who use their personal devices (Bring Your Own Device / BYOD) to conduct Hall business.

2. Volunteer & Personal Device Security (BYOD)
Any volunteer processing Hall documentation (such as hire contracts, invoices, or committee minutes) on a personal laptop, tablet, or phone must adhere to the following rules:

- **Device Access Controls:** Devices used for Hall business must be protected by a strong password, PIN, or biometric lock. Devices must never be left unlocked or accessible to family members or members of the public.
- **Security Software:** Volunteers must ensure their operating system (Windows/macOS) has automatic updates enabled and runs active, reputable anti-virus software.
- **Local Data Storage:** To prevent data leaks if a laptop is lost or stolen, volunteers must not download or store spreadsheets containing hirer contact details or financial information directly onto their personal hard drives. All work must be conducted within the official cloud platforms.

3. Shared Email (Outlook) & Cloud Storage (Google Drive)
The Hall relies on a shared Outlook email address and a shared Google Drive for records. To keep these environments secure:

- **Multi-Factor Authentication (MFA):** Two-Factor / Multi-Factor Authentication must be turned on for the shared Outlook and Google Drive accounts.

- **Password Management:** The passwords to these accounts must be complex and unique. They must never be shared with anyone outside the active committee.
- **Offboarding Volunteers:** Passwords to all shared accounts must be changed immediately whenever a trustee, bookings clerk, or volunteer steps down from their role.
- **Document Ownership:** All official committee minutes, financial records, and hiring contracts must be saved directly to the Hall's central Google Drive, rather than personal storage spaces.

4. Financial Controls & Invoice Integrity
To prevent phishing, invoice tampering, and fraudulent bank transfers:

- **Immutable Invoices:** All invoices sent to hirers must be generated and sent as uneditable PDF documents. Invoices must never be sent in Word or Excel formats.
- **Payment Detail Verification:** The Hall's bank details on the hire contract must match the details on the invoice exactly.
- **Dual Sign-off for Outgoings:** Any bank transfer or refund exceeding £[Insert Amount, e.g., 200] requires verbal or written confirmation from a second designated trustee before the transaction is processed.

5. Public Wi-Fi Terms of Use
The Hall provides public Wi-Fi for the convenience of hirers. To mitigate legal and digital risk:

- **Network Separation:** If technically possible, the guest Wi-Fi must remain completely isolated from any smart devices used to run the hall (such as smart meters or digital thermostats).
- **Mandatory Booking Clause:** The following clause must be included in all standard hiring agreements and signed by the hirer:"Wi-Fi is provided free of charge for lawful guest use only. The Village Hall Committee takes no responsibility for data loss, intercept, malware, or third-party device security while connected to the network. Illegal downloads, cyber-attacks, or malicious network activities are strictly prohibited and will result in access being permanently blocked."

6. Incident Reporting
If a volunteer suspects a security breach—such as a misplaced laptop containing Hall data, a compromised password, or a phishing email that was accidentally clicked—they must report it to the [Chair/Secretary] within 24 hours.

The committee will then review whether the breach requires reporting to the Information Commissioner's Office (ICO) under UK data protection regulations.

Volunteer Declaration:
I have read, understood, and agree to abide by the Beckley Village Hall Cyber & Data Security Policy.

Volunteer Name: _____
Signature: _____
Date: ____ / ____ / _____
