Holybrook Parish Council

Proudly serving the residents of Holybrook Parish since 2000

The Parish Office
Beansheaf Community Centre
Charrington Road
Calcot
Reading RG31 7AW

Tel: 0118 9454339
e-mail: clerk@holybrook-pc.gov.uk
www.holybrook-pc.gov.uk

Information Technology (IT) & Information Security Policy

Purpose

This policy sets out how Holybrook Parish Council manages its IT systems, devices, software and data in compliance with Assertion 10 of the *Smaller Authorities Proper Practices Panel Practitioner Guide 2025*, the UK GDPR, the Data Protection Act 2018 and the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018.

It provides a framework for IT security, data protection, accessibility and cyber-resilience across all council operations.

Scope

This policy applies to:

- All councillors, employees and contractors using council-owned IT systems or personal devices for council business.
- All hardware, software, email, online services and digital records used by the Council.
- Council-issued devices (including laptops) as detailed in *Appendix A – Councillor Laptop Policy 2025.*

Roles and Responsibilities

- **Council (as corporate body):** adoption, oversight and annual review.
- **Clerk:** day-to-day IT security, reporting breaches, managing access, ensuring backups, liaising with IT support. This includes delegation to the staffing team where appropriate.
- **All users:** compliance with this policy, immediate reporting of incidents and completion of mandatory training.

IT Equipment & Use

- Council will provide IT equipment where practical.
- Where personal devices are used for council business, they must:
- use strong passwords and automatic locking;
- remain up-to-date with security patches and anti-virus protection;

- not be shared with family or third parties for council work.
- Only licensed and authorised software may be used.
- Councillor-issued laptops are subject to the detailed provisions set out in *Appendix A – Councillor Laptop Policy 2025*, which must be signed and accepted before issue.

Email & Communications

- All council business must be conducted via official council accounts (e.g. forename.surname*@holybrook-pc.gov.uk*).
- Personal email accounts must not be used for council work.
- Spam and phishing awareness training will be undertaken by all staff and members.
- Email content and records are subject to Freedom of Information (FOI) and data protection legislation.

Data Protection & Confidentiality

- Personal data must be processed lawfully, fairly, securely and only for council purposes.
- The Council's Data Protection Policy, Privacy Notice and Retention Policy apply at all times.
- Personal data must not be stored indefinitely; retention schedules must be followed.
- Councillors and staff must respect confidentiality obligations at all times.

Access Control

- User accounts will be unique and not shared.
- Access rights will be reviewed at least annually and revoked when no longer required.
- Strong passwords and multi-factor authentication (MFA) will be used wherever supported.
- The Clerk maintains a register of user accounts and device allocations.

Backups & Continuity

- All critical data will be backed up at least weekly and stored securely (encrypted if cloud-based).
- Periodic restore tests will verify recoverability.
- An IT continuity plan will be maintained for system-failure scenarios.

Website & Accessibility

- The council website must comply with WCAG 2.2 AA standards.
- An Accessibility Statement will be published and reviewed annually.
- Where documents are not accessible (e.g. scanned PDFs), alternative formats will be provided on request.
- Progress on fixing accessibility issues will be reported to Council.

Security & Incident Management

- Incidents (loss/theft of devices, malware infection, data breach) must be reported to the Clerk immediately.
- Data breaches will be logged and assessed per ICO guidance.
- Where required, breaches will be reported to the ICO within 72 hours.

- Councillors must follow *Appendix A* for laptop-specific incident procedures.

Training

Councillors and staff will undertake mandatory training on:

- Data protection (every 2 years)
- Cybersecurity & phishing awareness (annually)
- Accessibility awareness (at induction and as updates occur)

Monitoring & Review

- This policy will be reviewed annually by full council and updated to reflect changes in law, SAPPP guidance or council needs.
- Non-compliance may result in disciplinary or governance action.
- Adoption and review will be recorded in Council minutes.

Adopted Monday 10th November 2025; V1_Reviewed annually

Appendix A – Councillor Laptop Policy 2025

Purpose

This appendix sets out the terms and conditions for use of laptops issued by Holybrook Parish Council to councillors. Devices are provided solely to facilitate efficient communication, secure record-keeping and effective participation in council business.

Scope

Applies to all parish councillors issued a laptop by the Council. Use is conditional upon signing the acceptance form attached to this policy.

Permitted Use

Council-issued laptops may be used only for council business, including:

- accessing and responding to council emails;
- preparing for and attending meetings;
- reviewing and storing council documents;
- research or communications related to council matters.
  Personal use is not permitted.

Prohibited Use / Misuse

Misuse includes, but is not limited to:

- Accessing, viewing, storing or distributing inappropriate, offensive or illegal material.
- Using the laptop for personal or commercial gain.
- Allowing third parties (including family) to use the device.
- Installing unauthorised software or altering system settings.
- Taking the laptop abroad.
- Gambling, gaming or political campaigning.
- Bringing the Council into disrepute (see Social Media Policy).
-

Any suspected misuse may lead to withdrawal of the device and further action.

Data Protection & Security

Councillors must:

- Keep the device password-protected (password shared with the Clerk only).
- Not share login credentials.
- Comply with the Data Protection Act 2018, GDPR and Council policies.
- Report any data breach immediately to the Clerk.
- Lock or shut down the laptop when unattended.
- Never leave it visible in vehicles or public places.
- Remain alert to spam/phishing emails.

- Store data in accordance with the Council's Retention Policy.
- Use council email accounts exclusively for council business.
- Not store confidential information on external media unless encrypted and authorised.
- Avoid unsecured public Wi-Fi; use a VPN where possible.

Care and Maintenance

- Councillors must take reasonable care of the laptop.
- Faults, damage or suspected security issues must be reported immediately.
- Repairs for normal use are covered by the Council; negligence may incur charges.
- Routine maintenance and updates will be managed by the Council's IT provider.
- Laptops are insured within the UK (does not cover accidental or negligent damage).
- Theft must be reported to the police and Clerk immediately with a crime reference number.

Return of Equipment

Laptops and accessories remain Council property and must be returned:

- at the end of office, resignation or disqualification; or
- when requested due to misuse or change in circumstances.
  Devices must be returned in good condition, allowing for normal wear and tear.

Monitoring and Compliance

The Council may monitor device use to ensure compliance. Breaches may result in withdrawal of equipment or other action consistent with governance procedures.

Policy Agreement

By accepting a Council-issued laptop, councillors agree to abide by this Appendix and the overarching Information Technology & Information Security Policy.

No laptop will be issued without a signed acceptance form.