



Information Technology (IT) Policy for Otterford Parish Council

Purpose

This policy governs the secure, efficient, and compliant use of Information Technology (IT) systems by Otterford Parish Council to support its functions, including local planning evaluations, accounting, maintenance of parish facilities, environmental responsibilities, and community engagement. It ensures compliance with UK legal requirements, including UK GDPR and the Data Protection Act 2018, while addressing the council's limited resources and rural context.

Scope

This policy applies to all Otterford Parish Council members, employees, volunteers, and contractors who use council IT systems, including computers, email, websites, and cloud services. It covers hardware, software, data storage, and communication tools used for council business.

Principles

1. **Security:** Protect council data and systems from unauthorised access, loss, or breaches.
2. **Compliance:** Adhere to UK GDPR, the Data Protection Act 2018, and NALC guidelines.
3. **Accessibility:** Ensure IT systems are user-friendly for council members with varying technical skills.
4. **Cost-Effectiveness:** Prioritise affordable solutions suitable for a small parish council.
5. **Transparency:** Maintain clear records of IT usage for accountability to residents.

IT Systems and Usage

1. **Hardware:**
 - The council uses a limited number of devices (e.g., laptops or tablets) for administrative tasks, primarily managed by the Parish Clerk.
 - Devices are password-protected and equipped with up-to-date antivirus software.
 - Personal devices used for council business must comply with this policy.
2. **Software:**
 - Approved software includes Microsoft Office (or equivalent, e.g., LibreOffice), email clients, and cloud-based tools like Microsoft Teams, as used by Somerset Council.

- Only licensed or open-source software may be installed on council devices.
 - Software for specific tasks, such as accounting packages, must be approved by the council.
3. **Email and Communication:**
- Official council email (e.g., clerk@otterfordparishcouncil.gov.uk) must be used for all council-related correspondence.
 - Emails containing personal data must be encrypted or password-protected.
 - Social media accounts (if used) must be managed by designated council members and comply with NALC's social media guidelines.
4. **Website:**
- The council's website www.otterfordparishcouncil.gov.uk must comply with the Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018.
 - Regular updates will ensure transparency, including publishing meeting minutes, agendas, AGAR and financial accounts.
 - The website must use secure hosting with SSL encryption.
5. **Cloud and Data Storage:**
- Data will be stored on secure, UK-based cloud services (e.g., Microsoft OneDrive) compliant with UK GDPR.
 - Physical storage devices (e.g., USB drives) must be encrypted and stored securely.
 - Backups will be performed monthly and stored separately from primary data.

Data Protection and Security

1. **Compliance with UK GDPR:**
- Personal data (e.g., resident contact details, planning application information) will only be collected with explicit consent and used for specific council purposes.
 - Data breaches must be reported to the Information Commissioner's Office (ICO) within 72 hours, as per UK GDPR requirements.
 - The Parish Clerk will act as the Data Protection Officer, responsible for data handling and ICO registration.
2. **Access Control:**
- Access to IT systems and data will be restricted to authorised personnel based on their role.
 - Passwords must be strong (minimum 12 characters, including letters, numbers, and symbols) and changed every six months.
 - Two-factor authentication (2FA) will be enabled where available.
3. **Cybersecurity:**
- Antivirus and firewall software must be installed on all council devices and updated regularly.
 - Council members will be trained to recognise phishing emails and other cyber threats, potentially through free resources from the National Cyber Security Centre (NCSC).
 - Suspicious activity must be reported to the Parish Clerk immediately.
4. **Data Retention:**

- Data will be retained only as long as necessary, in line with NALC's Document Retention Policy (e.g., financial records for 6 years, planning documents as required by Somerset Council).
- Obsolete data will be securely deleted or shredded.

Acceptable Use

1. Permitted Use:

- IT systems may only be used for council-related activities, such as drafting minutes, responding to resident queries, or analysing planning applications.
- Limited personal use of council email or devices is permitted, provided it does not interfere with council duties or violate this policy.

2. Prohibited Use:

- Installing unauthorized software or accessing inappropriate websites (e.g., gambling, illegal content) is strictly prohibited.
- Sharing council login credentials or sensitive data with unauthorised individuals is forbidden.
- Using IT systems for personal commercial activities is not allowed.

Training and Support

- Council members and volunteers will receive basic IT training, focusing on secure email use, data protection, and website management.
- Training may be sourced from Somerset Council's digital skills programmes, SALC training or other reliable sources.
- The Parish Clerk will serve as the primary point of contact for IT support, with external assistance sought as needed within budget constraints.

Maintenance and Upgrades

- IT systems will be reviewed annually to ensure they remain fit for purpose.
- Hardware will be replaced or upgraded as needed, subject to budget approval, prioritising cost-effective solutions (e.g., refurbished devices).
- Software updates will be applied promptly to address security vulnerabilities.

Monitoring and Compliance

- **Audits:** The Parish Clerk will conduct annual IT audits to ensure compliance with this policy and UK regulations.
- **Incident Reporting:** IT issues, including data breaches or system failures, must be reported to the Parish Clerk immediately.
- **Public Transparency:** A summary of IT usage and any incidents will be included in the council's annual report, available on www.otterfordparishcouncil.gov.uk

Budget and Resource Constraints

- Given Otterford's small population (356) and limited funds, IT solutions will prioritize low-cost or free tools.

- Collaboration with Somerset Council will be sought for shared IT resources or expertise.

Legal and Ethical Compliance

- **Accessibility:** All digital services, including the council website, will comply with the Public Sector Bodies Accessibility Regulations 2018.
- **Freedom of Information:** IT systems will support compliance with the Freedom of Information Act 2000, ensuring records are accessible upon request.
- **Ethical Use:** IT systems will not be used for activities that could harm residents' trust, such as unauthorised data sharing or surveillance.

Review and Feedback

- This policy will be reviewed annually at the Annual Parish Council Meeting or as required by changes in legislation.
- Residents may provide feedback on IT-related matters via the Parish Clerk. clerk@otterfordparishcouncil.gov.uk
- Updates to this policy will be published on the council website.

Approval

This policy was approved by Otterford Parish Council on Tuesday 12th August 2025 and is effective immediately. For enquiries, contact the Parish Clerk at clerk@otterfordparishcouncil.gov.uk

Prepared by Helen Andrew, Parish Clerk

August 5th 2025