Version	Description of Change	Officer	Reviewing Committee	Frequency of Review	Version Approval Date	Next Review Date
1.	Creation of policy	Parish Clerk	Full Council	Annual	10/02/2026 Min Ref: FC/100226/15 (2)	10/02/27

Burwell Parish Council
IT Policy

This document is based on the template provided by the Smaller Authorities' Proper Practices Panel (SAPPP). It is provided to help smaller authorities meet the requirements set out in the 2025 Practitioners' Guide. Assertion 10 (Digital and Data Compliance) requires all smaller authorities to adopt a formal IT policy. This template supports councils in setting clear expectations for how Clerks, Councillors, and staff should use digital systems, devices, and software securely and legally, whether on council-owned or personal equipment.

Introduction

Burwell Parish Council (the Council) recognises the importance of effective, reliable and secure information technology (IT) and email systems in supporting its statutory functions, decision-making, service delivery and communications.

This policy sets out the standards, responsibilities and acceptable use requirements for IT equipment, systems and email provided or used on behalf of Burwell Parish Council.

Scope

This policy applies to: - All councillors of Burwell Parish Council - The Parish Clerk, Responsible Financial Officer (RFO) and any other employees - Contractors, consultants and volunteers who access Council IT systems or data

It covers all Council-owned or Council-approved: - Computers, laptops and mobile devices - Networks and internet connections - Software and applications - Data and information systems - Email accounts and cloud-based services

---

Version	Description of Change	Officer	Reviewing Committee	Frequency of Review	Version Approval Date	Next Review Date
1.	Creation of policy	Parish Clerk	Full Council	Annual	10/02/2026 Min Ref: FC/100226/15 (2)	10/02/27

Acceptable Use of IT Resources and Email

Council IT resources and email accounts must be used primarily for official Council business.

Limited personal use may be permitted provided that it: - Does not interfere with Council duties or working time - Does not incur additional cost to the Council - Does not breach this policy or any other Council policy

Users must: - Act professionally and lawfully at all times - Respect copyright, licensing and intellectual property rights - Not access, create, store or transmit material that is offensive, defamatory, discriminatory or unlawful.

Devices and Software

Where possible, IT equipment, software and applications will be provided or approved by the Council.

Users must not: - Install unauthorised software or applications on Council devices - Alter security settings or system configurations without permission - Use personal software or devices for Council business unless explicitly authorised by the Clerk/RFO

These controls are necessary to protect Council systems and data from security risks.

All councillors, employees, and other authorised users must lock their devices when leaving their desks to prevent unauthorised access. This applies to all council and personal devices used for work. Failure to comply may lead to further action/disciplinary action.

Data Management and Information Security

All Council information must be handled in accordance with: - The Data Protection Act 2018 - UK GDPR - The Council's Data Protection and Information Governance policies

Users must: - Store and transmit sensitive or confidential data securely using approved systems - Ensure appropriate backups are maintained where required - Use secure methods for the disposal or destruction of data and equipment

Version	Description of Change	Officer	Reviewing Committee	Frequency of Review	Version Approval Date	Next Review Date
1.	Creation of policy	Parish Clerk	Full Council	Annual	10/02/2026 Min Ref: FC/100226/15 (2)	10/02/27

Network and Internet Use

The Council's network and internet access must be used responsibly for Council purposes.

Users must not: - Download or share copyrighted material without appropriate permission - Use Council systems for illegal activities - Access websites that pose a security or reputational risk to the Council

Email Use and Standards

Council-provided email accounts must be used for all Council business and communications. No Council communications should be made from your personal email addresses.

Emails must: - Be written in a professional, courteous and appropriate tone - Accurately reflect Council decisions and positions - Not be used for party-political purposes

Confidential or sensitive information must not be sent by email unless appropriate security or encryption measures are in place.

Users must remain vigilant against phishing, malware and scams and should: - Verify senders before opening attachments or links - Report suspicious emails immediately

Passwords and Account Security

Users are responsible for the security of their accounts.

Passwords must: - Be strong and unique - Not be shared with others - Be changed regularly or immediately if compromise is suspected

Version	Description of Change	Officer	Reviewing Committee	Frequency of Review	Version Approval Date	Next Review Date
1.	Creation of policy	Parish Clerk	Full Council	Annual	10/02/2026 Min Ref: FC/100226/15 (2)	10/02/27

Mobile Devices and Remote Working

Where Council business is conducted remotely or on mobile devices, users must: - Use passcodes or biometric security - Ensure devices are not accessible to unauthorised persons - Apply the same standards of care as when working in the Council office

All devices containing council information must be stored safely and securely when not in use, i.e. when travelling, when working from home or councillors/employees own devices. Portable equipment (unless locked in a secure cabinet or office) should be kept with or near the user at all times; should not be left unattended when away from council premises and should never be left on view in parked vehicles.

Loss or theft of any device used for Council business must be reported immediately to the Clerk.

Monitoring and Privacy

The Council reserves the right to monitor the use of IT systems and email accounts to: - Ensure compliance with this policy - Protect Council systems and data - Meet legal and regulatory obligations

Any monitoring will be carried out lawfully and proportionately in accordance with data protection legislation.

Retention and Archiving

Emails and electronic records must be retained and archived in line with: - Legal requirements - The Council's retention schedule

Users should regularly review and delete unnecessary emails and files in accordance with these requirements.

Reporting Security Incidents

All suspected or actual IT or information security incidents must be reported immediately to the Parish Clerk or designated IT contact.

Version	Description of Change	Officer	Reviewing Committee	Frequency of Review	Version Approval Date	Next Review Date
1.	Creation of policy	Parish Clerk	Full Council	Annual	10/02/2026 Min Ref: FC/100226/15 (2)	10/02/27

This includes: - Data breaches or loss - Phishing or malware incidents - Unauthorised access to systems or information

---

Training and Awareness

The Council will provide guidance and training, as appropriate, to ensure councillors and staff understand: - IT security responsibilities - Data protection requirements - Safe use of email and digital systems

---

Councillor-Specific Responsibilities

In addition to the general requirements of this policy, councillors of Burwell Parish Council have specific responsibilities arising from their elected role.

Councillors must: - Use Council email accounts only for legitimate Council business - Ensure that communications accurately reflect Council decisions and do not purport to represent the Council unless properly authorised - Take particular care when handling personal data, confidential information and commercially sensitive material - Comply with the Members' Code of Conduct, including obligations relating to confidentiality, respect and proper use of resources - Ensure that Council equipment, documents and electronic information are kept secure and are not accessed by unauthorised persons.

Councillors should be mindful that emails and electronic records may be subject to public access requests, audit, investigation or disclosure under data protection or freedom of information legislation.

Compliance and Breaches

Failure to comply with this policy may result in: - Withdrawal or restriction of IT access - Investigation under relevant Council procedures - Further action where appropriate

---

Version	Description of Change	Officer	Reviewing Committee	Frequency of Review	Version Approval Date	Next Review Date
1.	Creation of policy	Parish Clerk	Full Council	Annual	10/02/2026 Min Ref: FC/100226/15 (2)	10/02/27

Policy Review

This policy will be reviewed annually or sooner if required due to changes in legislation, technology or Council operations.

Contact

For IT-related queries or to report incidents, contact the **Parish Clerk,** Burwell Parish Council. burwellpc@burwellparishcouncil.gov.uk 01638743142