Singleton and Charlton Parish Council

IT and Email Policy

This policy was adopted by Singleton & Charlton Parish Council (S&CPC) at its full council meeting on 3rd June 2026.

Introduction

Singleton & Charlton Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

Scope

This policy applies to all individuals who use IT resources, including computers, networks, software, devices, data, and email accounts. The Council endeavors to provide digital devices but acknowledges that some staff and members may be using their own personal devices. Everyone must adhere to this policy to maintain digital security.

Training and awareness

The Council will source regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. You should engage in regular training on email security and best practices, including but not limited to:

- the Parish Council Domain Helper Service's virtual cybersecurity workshops for councils;
- the National Cyber Security Centre Cyber Security training for small organisations and free Cyber Action Toolkit.

Acceptable use of council-provided IT resources and email

When using IT resources for the council's purposes, you must adhere to ethical standards, and respect copyright and intellectual property rights.

Where possible, authorised devices, software, and applications will be provided by the Council for work-related tasks.

You must not install unauthorised software without checking with the Clerk, and you must not use equipment or email to access or forward inappropriate or offensive content.

Confidentiality

Some council business is confidential. This includes matters discussed in Part 2 of meetings (items from which the public and press are excluded), staffing matters, legal advice, commercially sensitive information, and personal data about identifiable individuals.

Confidential information must not be discussed, forwarded, copied, or stored outside official council systems. It must not be shared with family members, other councillors not party to the matter, or third parties. The obligation of confidentiality continues after a councillor leaves office or a member of staff leaves employment.

If you are unsure whether information is confidential, treat it as confidential and check with the Clerk.

What you must do if you use your own personal devices

The Council will endeavour to provide individuals with devices to use for council business. If you are using your own device you must make sure you are:

- using strong passwords for all your accounts (preferably using a password manager);
- downloading the latest operating system security updates;
- using anti-virus software.

Network and internet usage

Always use a trusted internet connection — your home network, a council-provided connection, or a mobile data tether — when carrying out official business. Avoid using public Wi-Fi in cafés, on trains, or in other public places, as these networks can be targeted by attackers. If you must use public Wi-Fi for council business, use a VPN.

Data storage and location

Council data should be stored on official council systems wherever possible. This means the council's email accounts, shared drive, and any council-provided cloud storage.

You must not store council data in personal cloud accounts (personal Dropbox, iCloud, personal Google Drive, etc.). Where council data must temporarily be held on a personal device, the amount should be kept to the minimum necessary, and the data deleted as soon as it is no longer needed.

Removable media (USB sticks, external drives) should be avoided. If used to carry council data, they must be encrypted and the data deleted once transferred.

Password and account security

You are responsible for maintaining the security of your accounts and passwords. Use the National Cyber Security Centre's advice for choosing a strong password. For business continuity, login details and passwords need to be stored securely so they can be accessed by trusted individuals in an emergency.

Email communication

The Council will endeavour to provide you with an official email account for organisation-related communication only. If you are currently using a personal email account, you should aim to move over to an official email account as soon as practically possible.

You must make sure that emails are professional and respectful in tone. You must always check you are sending any confidential or sensitive information to the correct recipients.

Always be cautious when downloading attachments and opening links to avoid phishing and malware. Before opening any attachments or clicking on links, verify the source by looking carefully at the email it has come from. Do not download and open anything if you are unsure who has sent it.

Email access and monitoring

The Clerk may need to access emails sent or received on council accounts to respond to Freedom of Information requests, subject access requests, audit queries, or to maintain business continuity (for example, where a councillor or member of staff is unavailable).

For employees, the Council may monitor email content where there is a legitimate business reason to do so, in accordance with the Data Protection Act 2018, UK GDPR, and the Council's separate Data Protection Policy.

If you use a personal email account for council business, the emails you send and receive on council matters remain subject to data protection law and may fall within the scope of FOI or subject access requests. This is one of the reasons councillors and staff should use official council email accounts wherever possible.

Social media

Social media includes blogs; Wikipedia and other similar sites where text can be posted; multimedia or user-generated media sites (YouTube); social networking sites (such as Facebook, LinkedIn, X (formerly known as Twitter), Instagram, TikTok, etc.); WhatsApp; text messaging and mobile device communications; and more traditional forms of media such as TV and newspapers. Care should be taken when using social media at any time, either using council systems or at home.

Inappropriate comments and postings can adversely affect the reputation of the council, even if it is not directly referenced. If comments or photographs could reasonably be

interpreted as being associated with the council, or if remarks could be regarded as abusive, humiliating, sexual harassment, discriminatory or derogatory, or could constitute bullying or harassment, the council will treat this as a serious disciplinary offence.

Councillors, staff, and other authorised users should be aware that parishioners or other local organisations may read councillors', staff, and other authorised users' personal weblogs to acquire information, for example, about their work, internal council business, and employee morale. Therefore, even if the council is not named, care should be taken with any views expressed.

Data management and security

All sensitive and confidential data should be stored and transmitted securely. You must regularly back up any important data to prevent data loss.

Data retention

Council records must be retained and disposed of in accordance with the council's Document Retention Policy. Routine emails that are not council records (for example, duplicates, scheduling notes, social correspondence) should be deleted regularly to keep inboxes manageable. Records that form part of a council decision, transaction, or formal communication must be retained per the retention schedule, even if held only in email.

Leavers

When a councillor leaves office (by resignation, end of term, or otherwise) or a member of staff leaves employment:

- Their council email account will be suspended on their last day. The Clerk may retain access to the account for a period of up to **30 days** to handle outstanding correspondence and information requests, after which the account will be closed.
- Any council-owned devices, equipment, keys, or access cards must be returned to the Clerk within 7 days.
- Any council data held on personal devices, personal email accounts, or personal cloud storage must be deleted. The leaver will be asked to confirm in writing that this has been done.
- Access to shared drives, the council's password manager, social media accounts, the council website, and any other council systems will be revoked.
- All records created in the course of council business (emails, documents, photographs, minutes, working papers) remain the property of the council. They must not be retained, forwarded to personal accounts, or used after leaving.
- The duty of confidentiality (section 5) continues to apply after leaving.

Reporting security incidents

All suspected security breaches, including email breaches or incidents, should be reported immediately to clerk@singletoncharlton-pc.gov.uk.

Relationship to other policies

This policy should be read alongside the council's other policies.

Where any conflict arises, the Code of Conduct and Standing Orders take precedence for councillors; employment contracts and the Data Protection Policy take precedence for staff.

The Clerk acts as the council's data protection lead. Small parish councils are not required to appoint a formal Data Protection Officer, but the Clerk is the point of contact for data protection queries.

Compliance and consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges. For staff, breach may be treated as a disciplinary matter under the council's employment policies. For councillors, breach may be treated as a matter under the Code of Conduct.

Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

Contacts

For IT-related enquiries or assistance, users can contact clerk@singletoncharlton-pc.gov.uk.

All staff and councillors are responsible for the safety and security of IT and email systems.