

1. Introduction

The parish council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

This purpose of this policy is to ensure that all employees, councillors and any third parties using Sancreed Parish Council IT have a clear understanding of what is and is not permitted. This will ensure the appropriate use of the Council's equipment, safeguard the security of its IT systems and data, and assist compliance with any relevant legislation.

2. Definitions

Users – councillors, employees and third parties acting on behalf of the Council

Data – digitally stored information including (but not limited to) documents and copyrighted/copyrightable text, images, personal information, accounting information.

IT (Information Technology) – includes, but is not limited to, computers, internet access, remote access connections, email servers, file storage, webmail, smart phones, telephones, website, mobile phones etc

3. Scope

This policy applies to all users of the parish council's IT resources, including third parties and contractors.

4. Acceptable use of IT resources and email

Computer access

Access to the council's IT systems is controlled by the use of user ID's and passwords. Individuals must not:

- leave their user accounts logged in at an unattended and unlocked computer
- leave their password unprotected
- perform any unauthorised changes to the IT systems or information
- attempt to access data that they are not authorised to use or access
- connect any unauthorised device to the council's network or IT systems
- store council data on unauthorised equipment
- give or transfer council data or software to any person or organisation outside the council without the appropriate authority to do so.

Individuals must not store personal files, such as music, video, photographs or games, on council IT equipment.

Internet and email conditions of use

The council's internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to the council in any way, not in breach of any terms and conditions of employment and does not place the individual or the council in breach of statutory or any other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Internet access unacceptable behaviour

In particular, the following is deemed unacceptable use or behaviour

- visiting sites that contain obscene, hateful, pornographic or illegal material
- perpetrating any form of fraud, or software, film or music piracy
- using the internet to send offensive or harassing material to other users
- downloading commercial software or any copyrighted materials belonging to third parties, unless the download is covered or permitted under a commercial agreement or other such licence
- hacking into unauthorised system, sites or files
- publishing defamatory and/or knowingly false information about the council, colleagues, Members and/or customers on social networking sites, blogs, wikis or any online publishing format
- revealing confidential information about the council in a personal online posting, upload or transmission; including financial information and information relating to employees, Members and/or internal discussions
- introducing any form of malicious software into the council network

Email usage unacceptable behaviour

In particular, the following is deemed unacceptable use or behaviour:

- distributing, disseminating or storing images, text or materials that are illegal, or might be considered indecent, pornographic or obscene
- distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered harassment
- use of council communications systems to set up personal businesses or send chain letters
- forwarding council confidential messages to external locations
- accessing copyright information in a way that violates the copyright
- broadcasting unsolicited personal views on social, political, religious or other non-council related matters or transmitting unsolicited commercial or advertising material.

Emails should not be kept longer than they are required in line with our Data Protection Policy.

Users should be aware of the characteristics of spam and phishing emails and should not reply to these emails, but add the sender to the email system's blocked senders list.

Actions upon termination of contract of employment, or cessation of term of office of councillors

All council equipment and data, for example laptops and mobile devices, must be returned to the council when employees / councillors leave the council.

5. Device and software usage

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

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

6. Data management and security

All sensitive and confidential the parish council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

9. Password and account security

The parish council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

10. Mobile devices and remote work

Mobile devices provided by the parish council should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office.

11. Email monitoring

All data that is created and stored on council computers is the property of the council and there is no official provision for individual data privacy. However, where possible the council will avoid opening personal emails.

The council maintains the right to examine any systems and inspect any data recorded in those systems, which includes but is not limited to internet access and email or messaging content. As a matter of compliance with this policy and meeting the regulatory requirements asked of the council, the council reserves the right to use monitoring software in order to check upon the use and content of emails. The council maintains the right to monitor the volume of internet and network traffic, together with internet sites visited. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Any monitoring will be carried out in accordance with audited, controlled internal processes, current UK Data Protection law, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000. Any individuals who suspect a breach of security policy must report it without delay to the Clerk/RFO. All breaches of information security policy will be investigated and where investigations reveal misconduct, disciplinary action may follow in line with disciplinary procedures. Breaches of the IT Policy by Members could contravene the Code of Conduct and action may result from this contravention.

12. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

13. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately.

14. Reporting loss or theft

In the event of loss or theft of any mobile device, irrespective of whether it is council-issued or personally owned, the user must act promptly to minimise the risk of compromise to council information by immediately:

- reporting theft of device to the police (if stolen)
- reporting the theft or loss to the Clerk / Chair, as appropriate
- changing any passwords that may have been used on the device, eg banking

15. Training and awareness

The parish council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive regular training on email security and best practices.

16. Compliance and consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

17. 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.

18. Contacts

For IT-related enquiries or assistance, users can contact the Clerk/RFO.

All staff and councillors are responsible for the safety and security of the parish council's IT and email systems. By adhering to this IT and Email Policy, the parish council aims to create a secure and efficient IT environment that supports its mission and goals.

Date: _____

Signature: _____

Role: _____