

Sheet Parish Council

Information Technology and Email Policy

Introduction

Sheet Parish Council has a duty laid down in the Data Protection Act 2018, to ensure the proper security and privacy of its computer systems and data - this is complicated by the majority of devices belonging to individuals and not to the Council. Good practice as outlined here applies equally to Council assets and private devices. All users have, to varying degrees, some responsibility for protecting these assets. Users also have a personal responsibility for ensuring that they comply fully with this policy.

The Clerk and Responsible Finance Officer is responsible for the implementation and monitoring of this policy and has a responsibility to ensure that all staff and councillors using IT equipment comply with this policy.

General Principles

The policy applies to the following aspects of ICT including personal devices:

- Computers and Laptops
- Remote Access Connections
- Mobile Phones and Tablets
- Emails and Email Servers
- Portable Devices
- Internet Access
- Website and Social Media
- Passwords
- Viruses
- Software
- Cyber Security
- Training

All users of IT equipment must be familiar with and abide by the regulations set out in the council's 'Data Protection & GDPR Policy'.

All users are reminded that deliberate unauthorised use, alteration, or interference with any computer system, software or data is a breach of this policy and in most circumstances will be a criminal offence under the Computer Misuse Act 1990.

All software installed on devices, whether provided by the council or a personal device must be fully licensed and no software should be installed on any council provided equipment without authorisation from the Clerk and Responsible Finance Officer.

Passwords and Password Protection

All computers and systems must be password protected to prevent unauthorised access.

- Where possible, two factor authentication should be utilised.
- Users should ensure that unattended devices are password protected.

As a rule, users will never be asked to share passwords by email

- Where users have unique access permissions and/or accounts for systems, these must not be shared with other users.
- Different passwords should be used for different devices and accounts.
- Passwords should be secure and changed immediately if there is any possibility of a breach.
- Passwords should not be written down or left in unsecure locations.
- Passwords must not be inserted into email messages or any other form of communication or saved onto a shared computer.

Security and Virus Controls

All devices, including personal devices, should have up-to-date antivirus software installed and this must not be switched off for any reason. Such software is usually provided with the operating system and does not require purchasing but be wary of “free” offers.

- Consideration must be given to the secure location of equipment and documentation to help safeguard Sheet PC's ICT assets, as well as personal devices. Portable equipment must be locked away when not in use and must not be removed from the premises without permission.
- Only those authorised by the Clerk and Responsible Finance Officer may use Sheet PC's computer systems. The authority given to use a system must be sufficient but not excessive and users must be notified that the authority given to them must not be exceeded.
- Operating procedures are required to control use of ICT equipment.
- Security incidents relating to any aspect of this policy must be reported to the Clerk and Responsible Finance Officer immediately.
- Avoid using public wi-fi connections that are not secure.

Virus Controls

- Viruses are undesirable pieces of computer code that can corrupt systems, equipment, and data. They are a serious, increasing threat to the computer systems of Sheet PC.
- If a virus is suspected, the equipment should be switched off and isolated and Sheet PC's support contractor should be contacted.
- Viruses are easily transmitted via email and internet downloads. In particular users must:

IT Policy (version1)

- not transmit by email any file attachment which they know to be infected with a virus.
- not download data or programs of any nature from unknown sources
- not forward virus warning
- report any scam emails that arrive using the email self-reporting tool. If the load becomes excessive inform Sheet PC's IT providers.
- No software should be located onto Sheet PC's equipment without the permission of the Clerk and Responsible Finance Officer.

Computer use

- Laptops/Computers should be shut down at the end of every day and kept in a secure locked drawer/cabinet if left in the office.
- Laptops/Computers should be secure and out of reach of the public and logged out when a member of staff is away from their desk.

Use of E-mail

E-mails sent or received form part of official records of Sheet PC- they are not private property. E-mails may be disclosed under the Freedom of Information Act, as part of legal proceedings (e.g. tribunals) and as part of disciplinary proceedings.

Employees are responsible for all actions relating to their e-mail accounts/username and must ensure that no other person has access to their account without the permission or knowledge of the Clerk and Responsible Finance Officer.

When using Sheet PC e-mail, employees must:-

be aware of odd language used in emails which may indicate a fraudulent email.

- Correctly maintain their own e-mail folders and delete all unwanted mail on a regular basis.
- Not use e-mail for the creation, retention, or distribution of disruptive or offensive messages, images, materials, or software that includes offensive or abusive comments about ethnicity, nationality, gender, disabilities, age, sexual orientation, appearance, religious beliefs and practices, political beliefs, or social background.

Employees who receive e-mails with this content must report the matter to the Clerk and Responsible Finance Officer.

- Not send e-mail messages that might be considered by the recipients as bullying, harassing, abusive, malicious, discriminatory, defamatory and libelous or containing illegal or offensive material or foul language
- Not upload, download, use, retain, distribute, or disseminate any images text materials or software which might reasonably be considered indecent, obscene, pornographic, or illegal.
- Not engage in any activity that is outside the scope of normal work-related duties.
- Not send chain-letters or joke e-mails

- Personal use of Sheet PC e-mail is NOT permitted without the prior permission of the Clerk and Responsible Finance Officer.

Document Storage

All Council documents should be stored in OneDrive or, when implemented, SharePoint. Such folders can be synchronised with one's access device, but under no circumstances should any document be stored in personal folders such as "My Documents"

Use of the Internet

Even when acting in a personal capacity, councillors and employees should not:-

- Participate in any on-line activity that would bring Sheet PC into disrepute.
- Visit, view, or download any material from an internet site which contains illegal or inappropriate material.
- Knowingly introduce any form of computer virus into Sheet PC's computer network.
- Download commercial software or any copyright material belonging to third parties unless agreed.
- Abuse of these procedures could lead to disciplinary action being taken.

Cyber Security

Implementing effective ICT security measures is a key part of safety controls and risk management of running Sheet PC. All users should be aware of the increasingly sophisticated scams and risks posed to cybersecurity and when in any doubt should seek guidance from the Clerk and Responsible Finance Officer.

- Current and up to date information should be shared with all Staff and Councillors.
- Cyber Security must be included as part of Sheet PC's Risk Management Policy.
- The council will regularly review the benefits/cost of achieving Cyber Essentials Certification and the Cyber Insurance that comes with it.

Training

Employees and Councillors should be provided with regular cybersecurity awareness training as is appropriate for their role and level of systems access and be made aware of the risks of email security as part of their induction process.

Monitoring and misuse of I.T

Misuse includes, but is not limited to:

- Creation or transmission of any offensive, obscene or indecent images, data or other material or any data capable of being resolved into obscene or indecent images or material.
- Creation of material which is designed or likely to cause annoyance, inconvenience, or needless anxiety.

IT Policy (version1)

- Creation or transmission of defamatory material
- Transmission of material which in anyway infringes the copyright of another person.
- Transmission of unsolicited commercial advertising material to networks belonging to other organisations
- Deliberate actions or activities with any of the following characteristics:
 - i. Wasting staff effort or networked resources
 - ii. Corrupting or destroying another users' data.
 - iii. Violating the privacy of other users.
 - iv. Disrupting the work of other users.
- Other misuse of the networked resources by the deliberate introduction of viruses/malware
- Altering the setup or operating perimeters of any computer equipment without authority.
- Unauthorised access, use, destruction, modification and/or distribution of council information, systems or data is prohibited.

Monitoring the use of the council's email and document storage may take place if breaches of use are believed to have occurred or to comply with the law.

Misuse of IT facilities and not adhering to this policy could potentially result in disciplinary proceedings in line with the Sheet PC Disciplinary Policy.

Additional Information

For further guidance and information visit the National Cyber Security Centre website:

<https://www.ncsc.gov.uk/collection/board-toolkit/toolkits-toolbox>

[Public sector - NCSC.GOV.UK](https://www.ncsc.gov.uk/public-sector)

10th March 2026