

COMPUTER SYSTEMS CODE OF PRACTICE

1. Introduction and background

Parish Council relies almost without exception on its computer and communications facilities to carry out its business. All these facilities can be put at risk through improper or ill-informed use and result in consequences which may be damaging to individuals and their research, the Parish Council community and to establishment and reputations. Accordingly, this Code of Practice ("CoP" hereafter) aims to provide clear guidance to all employees concerning the use of Parish Council computer and communications facilities. It provides a framework of guidance, including individual responsibilities, to enable employees to use Parish Council's facilities with security and confidence and in line with best practice. Because of the importance that we attach to this area every employee is required to read, make themselves fully familiar with and comply with the Code of Practice, JANET (ja.net) Acceptable Use Policy and any relevant rules/local policies. This document is subject to any local rules/policies that may exist and should be read in conjunction with them.

2. Scope

This CoP applies to all Parish Council employees (i.e. permanent employees, temporary employees, contractors) provided with Parish Council computer and communications facilities and/or who use or gain access to:

- ◆ The Internet via the Parish Council wide area network and the connection to the academic and research network, JANET ("wide area network" hereafter) including Wireless hot spot facilities
- ◆ The Internet via an external connection but still using Parish Council equipment
- ◆ Any computing facility which is used in conjunction with Parish Council work
- ◆ Parish Council e-mail systems
- ◆ Parish Council telephone (assumed to include fax, voicemail and short messaging service [SMS]) systems

- ◆ Parish Council document production facilities

- ◆ Parish Council postal distribution facilities

Employees must ensure that they are aware of the relevant contents of the Security Policy by:

- ◆ Attending any required security training

- ◆ Abiding by the JANET Acceptable Use Policy

- ◆ Reading any relevant supplementary information published by Parish Council and disseminated to employees

The scope of this CoP does not cover oral conversations between individuals or groups of individuals. In addition, the use of photocopying or reprographic facilities is covered only to the extent to which such usage relates to the communications already within the scope of this policy.

Other codes of practice may be issued in support of the Security Policy and these will be complementary to this CoP.

3. Policy Statement

All Parish Council employees may make use of the provided computer and communications facilities to enable them to effectively conduct their work, as relevant. In particular such facilities can be used by employees to efficiently communicate with people within and outside the organisation and to gain access to information that will assist them in their work. Access is not given as of right. It is at management's discretion and may be withdrawn at any time.

This CoP, drawn up in support of the Security Policy, aims to reduce the likelihood of any legal liability arising against Parish Council employees and Parish Council itself and also contributes to ensuring that Parish Council can demonstrate effective and appropriate use of government resources.

The understanding and application of this CoP by employees will reduce the likelihood of breaches in security practices or regulations that could jeopardise the business and public reputation of Parish Council and its employees.

4. Responsibilities

All employees within the scope of this CoP are responsible for adhering to and implementing the Security Policies in force.

The Clerk to the Council and Head Steward are ultimately accountable for: adherence to legal requirements; Council policies, standards and procedures; ensuring that computer and communications facilities are used appropriately; and overseeing any disciplinary proceedings which may result from any form of misuse of provided facilities.

The day-to-day implementation of the Security Policy and its attendant procedures and practices is the particular responsibility of the Clerk to the Council, who may delegate responsibility for specific areas of the Security Policy to the Head Steward.

It is the responsibility of the Head Steward to ensure that the employees for whom they are responsible are fully conversant with their security responsibilities and that employees using any computer and communications facilities are properly trained in their use.

The Clerk to the Council is responsible for ensuring the maintenance, regular review and updating of this CoP. Revisions and amendments to the CoP will be implemented by joint agreement with the Parish Council, following change control procedures. Employees will be informed of any changes to the CoP via the employment code but some changes will require further formal signature by employees.

5. Disciplinary Procedures

Failure of employees to comply with the Security Policy and/or this CoP may result in disciplinary action up to and including dismissal, in accordance with Parish Council disciplinary provisions or codes, or in the case of contractors, termination of contracts and/or service agreements.

6. General use of Computer and Communications Facilities

All employees have a responsibility for ensuring the proper, economical, effective and efficient use of Parish Council resources within their control.

Standards for computer and communications equipment procurement are maintained by the Parish Council. All equipment and facilities within the scope of this CoP must be purchased in compliance with Parish Council standards. Computer workstations are installed in accordance with the standards defined by the Parish Council. Amongst other things, these define a standard computer workstation configuration (including, where relevant, the default browser home page). In terms of such configurations, employees are not permitted to change security settings (including browser settings) without first consulting with the Parish Council. Employees should never attach any device or equipment to the internal network without prior approval from the Parish Council.

Parish Council also provides landline telephone equipment for the use of employees. Employees must not disconnect their landline telephones without prior approval and must comply with the specific guidance that is issued for telephone use. Employees must also not install any telephone device without prior approval.

Employees are responsible for ensuring the physical security of Parish Council computer and communications facilities (including data) on-site, off-site and at home. Employees should pay particular attention to highly portable equipment, such as laptops, PDAs and mobile phones. Such equipment should be kept secured when not in use, even within the workplace. In general, Parish Council does not expect its employees to insure such equipment when off-site or at home, but employees must check local rules. However, employees should check their own domestic insurance conditions to ensure that the use of work equipment at home does not invalidate their policy.

Employees must inform the Head Steward of any loss of computer facilities.

Parish Council may also provide electronic templates for employees to use in the production of a range of documents e.g. official letters, internal memorandum, reports etc. Employees must use the templates where these have been provided.

Parish Council also provides systems and templates for the publication of documents onto intranets and websites. Parish Council has identified local individuals responsible for managing these systems and for controlling content. Employees must only publish information using the provided local systems and must furthermore ensure that the information published follows the specific editorial policies and/or guidance issued by the appropriate content manager. Where an employee has any doubt about publication, the relevant content manager must be consulted.

During planned absences, employees must use the 'out-of-office' facility to make others aware they are absent from work.

On leaving Parish Council employment, employees must return all Parish Council owned computer/communications equipment and data that has been issued to them. Employees must also return equipment and software licences upon the demand of the relevant asset manager.

6.1 Dealing with Inappropriate E-mails

If employees receive a misdirected e-mail they should respect the confidentiality of its contents, delete the e-mail and inform the sender unless the user believes any such e-mail contravenes the Security Policy or other Parish Council policy, guidance or code of practice in which case they should take no action except inform the Head Steward. Employees must not send a misdirected e-mail onto the likely intended recipient; this is the responsibility of the original sender.

If an employee receives defamatory, harassing or abusive e-mails, they must immediately inform the Head Steward. Employees must not respond to such e-mails.

7. Personal Use

This section covers purely non-work related communications and use. Employees should be aware that personal use of Parish Council computing facilities (e.g. e-mails and internet access) may impact upon Parish Council, and may be against local rules.

7.1 General Policies

Parish Council provides employees with access to computer and communications facilities so that they are able to effectively and efficiently undertake work duties. Employees are permitted to make limited and reasonable personal use of some of these facilities provided that such use is consistent with the guidance contained in this and other codes of practice and/or policies. Employees must not, however, use such facilities for personal financial gain unless prior approval from management has been received.

The facilities that employees are allowed to employ for personal use in the context of this policy are limited to their computer workstation and its network connection (including laptop/PDA), printers, software as permitted under the licensing arrangements, browsers, telephones and fax machines. Reasonable and limited use of Parish Council postal facilities for sending or receiving personal mail is also acceptable, provided the individual meets the full cost of the postage.

The nature of any personal use and the length of personal use will be important factors in determining whether such use is acceptable. Guidance on unacceptable use is given in later sections and guidance on length of use below.

7.2 Length of Personal Use

In this context “limited and reasonable” will depend on a number of factors including an individual’s objectives, the extent to which the personal use will conflict with official business, any demands that such use will place on Parish Council facilities and cost. For Parish Council employees most personal use (including telephone calls) should be undertaken in non-working time e.g. when clocked out at lunchtime. For employees contracted from or through an outside organisation, e.g. temporary employees provided by an agency, all personal use should be undertaken in non-work (non-chargeable) time.

In undertaking personal use, all employees should ask themselves questions including, but not limited to, the following:

- ◆ Would my actions be considered unacceptable if viewed by a member of the public?
- ◆ Would managers, auditors or others in similar positions call into question the cost effectiveness of either my use of work time or my use of Parish Council computer and communications facilities if they knew about it?
- ◆ Will my personal use have a negative impact upon the work or morale of my colleagues?
- ◆ Could my personal use bring Parish Council into disrepute?

- ◆ Is this usage in breach of my terms and conditions of employment?

Personal use should not be undertaken if the answer to any of these questions is 'yes'.

Responsibility for ensuring that any personal use is acceptable rests with the individual and with their line manager. Employees should contact their line manager if they have any doubts concerning the acceptability of their personal use. If any doubt still remains, then that form of personal use should not be undertaken.

7.3 Personal Files, Documents, E-mails and Telephone Calls

Employees are required to mark any personal e-mails they send with the word 'Personal' in the title line and to ask those they correspond with to similarly mark any personal e-mails being sent into Parish Council. Personal e-mails to be retained must be stored in folders clearly marked 'Personal'. Personal e-mails and folders should not be stored in Parish Council's electronic document or records facilities – they must only be stored within the areas designated for such storage by Parish Council. Any particularly sensitive files should be password protected. Parish Council is not responsible for the security and back-up of individuals' non-work data held on Parish Council computing facilities.

Individuals leaving a personal message on an employee's voice mail facilities should begin the message "This is a personal message for...".

Provided folders and documents are clearly marked as 'Personal' (as above) they will not be searched in the event of access for business continuity purposes. However, these files could be subject to access during legal investigation or potential breaches of Parish Council policies and codes. See also paragraph 10 and 12 of this appendix.

Personal hard copy documents should not be stored on any work files. Such documents may be kept in work storage facilities (e.g. desk pedestals) provided to the employee. The employee should further store these in a non-work folder or file that is clearly labelled 'Personal'. Maintaining the security of such documents is the sole responsibility of the individual.

When an employee leaves the organisation that person should ensure that all personal files, documents, e-mails, SMS messages and voicemails are removed or deleted. Any correspondence left on departure will no longer be considered personal. Mail marked personal, arriving after departure, will be returned to sender or destroyed.

An employee using a Parish Council-provided computer or communications facility for personal use is responsible for maintaining the confidentiality of that document, file or telephone call whilst it is being constructed or undertaken. Parish Council can take no responsibility for other employees viewing or hearing such communications.

8. Abuse and Misuse of Computer and Communications Facilities

This section provides specific guidance on use and abuse of Parish Council facilities. The section does not set out to be fully comprehensive and other abuses and misuses can be inferred from other sections in this document.

8.1 General Policies

Employees must not use Parish Council facilities to engage in any inappropriate or illegal activity. This includes, but is not limited to, knowingly viewing, accessing, producing, reproducing, storing, processing and/or distributing materials or messages that:

- ◆ contain pornographic content
- ◆ relate to criminal or terrorist skills or activities
- ◆ contravene Parish Council's equality and diversity policies
- ◆ is illegal in the UK – the downloading of transmission of indecent or obscene materials may amount to a criminal offence under the Obscene Publications Act 1959, the Protection of Children Act 1978, the Criminal Justice Act 1988 or the Communications Act 2003. Where Management believe that a criminal offence has been committed, they will immediately inform the Police and a prosecution may result
- ◆ is defamatory
- ◆ is indecent, offensive, obscene, or abusive
- ◆ is designed or likely to cause annoyance, inconvenience or needless anxiety, or wastes an employees effort and resources
- ◆ infringes copyright or other intellectual property laws
- ◆ contains unsolicited commercial or advertising material

- ◆ is designed or known to corrupt or destroy other users' data
- ◆ deliberately denies the use of services to other users
- ◆ infringes the data protection rights or privacy of any other individual
- ◆ could endanger the health and safety of any other individual
- ◆ is inconsistent with other policies and guidelines issued by Parish Council (e.g. harassment)
- ◆ contains a virus, worm, Trojan horse, trap-door program or any other form of malicious code

All Parish Council computer and communications facilities must never be used to gain, or attempt to gain, unauthorised access to the computer systems of other organisations or individuals. Furthermore, employees must not use computer facilities to gain or attempt to gain unauthorised access to Parish Council's own systems.

Employees must never impersonate any other user or person on computer facilities without appropriate authority. Where a user believes there to be a legitimate business need to do this, the Parish Council must be informed and approval given.

Employee must not deliberately access personally marked files or folders of other employees unless following Parish Council procedures for such access.

When considering the acceptability of their use, employees should again ask themselves the questions posed in paragraph 7 of this appendix. It is the responsibility of employees to check with their respective line managers if they are in any doubt as to the acceptability of their uses. Line managers may wish to discuss the matter with the Parish Council.

Employees should note specifically that they must not install any computer games and/or peer-to-peer software onto their workstations. Screen-savers are to be installed as per local rules.

On occasion, employees may be instructed to cease specific computer or communication tasks by the Head Steward. Employees must comply with such instruction.

The following sections provide specific additional guidance to supplement these general policies.

8.2 Internet Use

Employees should be aware that material that would contravene this CoP is unfortunately readily available on the Internet. It is recognised that such material can be unknowingly accessed and to

minimise such incidents, Parish Council employs software that denies access to some inappropriate sites. However, it is the clear responsibility of employees to ensure that their use remains consistent with Parish Council guidelines. The fact that the blocking software allows access to a site does not imply that Parish Council believes that site to be acceptable.

Downloading or streaming audio or video files for personal use is not permitted. Furthermore, when accessing such material for business use, employees must pay particular care to ensure they do not infringe copyright or other laws.

8.3 Software Installation

Parish Council operates specific approval policies to ensure that only appropriate software is installed on its computing facilities. These policies are designed to ensure that Parish Council is operating with properly licensed software and to avoid the potential security breaches (e.g. viruses and spyware) that can be associated with unknown software.

Employees must ensure that they fully comply with the relevant approval procedures.

If in any doubt, employees should contact the Head Steward before downloading or installing any software from the Internet.

8.4 Software Use

Guidance on which facilities are available for personal use has been given in section 7 but, in addition, intranet facilities may, under certain circumstances, be used to disseminate non-work related information. Employees should refer any questions in this respect to the Head Steward. All other personal use of Parish Council information systems is unacceptable and a serious breach of this code of practice.

Software must be used in accordance with any instructions and training that has been given to the employees member. Employees must consult the Head Steward if they are in any doubt concerning the acceptability of the manner in which they are using the software.

8.5 Web Based Personal E-mail Accounts

Employees must not access web-based personal e-mail accounts unless given prior approval by the appropriate person, as this opens up the data network to an increased risk of virus infection.

8.6 E-mail Attachments

Large attachments should be used with care because they can have a detrimental effect on data networks. Parish Council will establish policies for dealing with large attachments which may include

their quarantining or rejection. Employees are advised to contact the Head Steward for guidance on such policies.

8.7 Instant Messaging

Employees must not make use of Internet chat/instant messaging facilities unless given prior approval by the Parish Council, as this increases the risk of a security breach of the data network.

8.8 Telephones

Employees must not make personal calls to premium rate numbers or to international numbers using Parish Council telephone facilities. Personal calls to mobile phones may be made in emergencies or by arrangement with the Head Steward.

However, specific arrangements may apply for other types of mobile telephone call and users should check arrangements with the member of employees responsible for managing the provision of their phone. In the absence of further guidance, the general policies in this document apply.

8.9 Document Templates

Employees must never use Parish Council branded templates (including hard copy letter-headed paper) for non-Parish Council use.

9. Data Management of Business Communications and Transactions (including those containing personal information)

Parish Council business data and communications should primarily be stored on network facilities or systems (not on local PC drives). Such data and communications must be processed in accordance with agreed procedures for document and records management (the hyperlink is for Parish Council Office staff only - others should consult local rules).

Many business communications and transactions will include personal information. These are considered to be business transactions unless marked as personal. Some such communications will be of a sensitive nature. The overriding consideration when dealing with such communications is for employees to comply with the Data Protection Act 1998. Employees must make themselves aware of their responsibilities with regard to this Act, see: Data Protection Act 1998 (PDF 152KB).

Notwithstanding any provision within separate document and records management policies, sensitive electronic documents should be kept in clearly marked folders with folder level access security employed where possible to restrict access. Hard copy files (such as personal files) containing sensitive paper documents should be kept secure with access controlled and provided only to relevant employees. Hard copy business correspondence containing personal and/or sensitive information that is being sent should be appropriately sealed and marked appropriately as described in published guidance.

Employees are responsible for any data held on mobile devices such as laptops and PDAs. The length of time that confidential or sensitive data is held on such devices or stored on computer server as deleted data should be kept to a minimum and the use of additional file-level passwords should be considered. In order to meet the requirements of the fifth data protection principle, it is essential that an objective justification for on-going retention of confidential/sensitive personal information can be stated. Where such data is kept for statistical or historical purposes, the data should be rendered anonymous at the earliest opportunity. Sensitive personal information (as defined in the Data Protection Act) should not be taken off-site without appropriate authority from the Parish Council.

Employees are responsible for the security and back-up of any and all data held on the local drives of workstations.

Employees must not create databases containing personal information either to be held locally or on network drives without first consulting with and getting approval from the Parish Council.

Other people's personal information must not be published on news or discussion groups. In addition, employees must not enter into public correspondence, debate or publicly disclose information about any matter they are dealing with as part of their job without prior authorisation by their line manager.

10. Access to Work-related/Business Files and E-mails

Employees should principally receive and produce correspondence and documents as agents of Parish Council.

All documents stored in Parish Council hard copy files or within Parish Council electronic document or records management systems will be assumed to relate to Parish Council and its transactions.

Unless they are explicitly marked as personal or are contained in a folder marked as personal, all stored files and also all e-mails (including those e-mails that may still exist either opened or unopened in an e-mail inbox) will be assumed to relate to Parish Council and its transactions.

For business continuity purposes, it may be necessary for other employees or managers to access work related electronic files and messages, for example to cover illness or holiday absences, or upon termination of employment. In the latter case, it is expected that the employee and Head Steward will have made suitable arrangements regarding such data prior to the employee's departure. Neither e-mails nor files will be moved or deleted unless the employee has left the organisation. As part of these access arrangements, the Parish Council will not provide access to other members of employees of e-mails or files marked as personal or stored in folders marked as personal.

Employees who have been granted proxy access by a colleague must not deliberately open items labelled as personal or search through any personal directories.

The Head Steward has responsibility for dealing with hard copy mail that arrives for an individual. The Head Steward has authority to access mail, or to delegate access rights, to all mail that arrives for their employees that is not marked "private" or "personal". "Private" or "personal" items should be left unopened unless written authority from a director is obtained.

Stored voicemails or SMS messages will be assumed to be work-related unless they are indicated as being personal. Those reviewing voicemail messages should not knowingly listen to any personal messages.

11. Password and Systems Lockdown

Employees must not divulge their passwords or allow anyone else to use their account at any time. Employees must not use their work password for any other purpose.

Employees must ensure their computers are password-locked when left unattended, unless otherwise instructed by the Head Steward. Employees must also not store their internal passwords on any external device or media. For example, if using a third party machine and a prompt appears to remember the password this must be declined.

12. Monitoring and Investigations of Use and Misuse

In addition to the access to files described paragraph 10 of this appendix employees should be aware that their use of Parish Council computer and communications systems is automatically logged and monitored in order to prevent unauthorized use of the system. Furthermore, detailed investigations of files, computers and communications activity may be undertaken where a specific need has been identified. These processes are described below.

- ◆ Internet usage: addresses of sites/pages accessed, date and time of access time, downloaded files
- ◆ E-mail: e-mail addresses of all correspondence, date and time of correspondence, message title. E-mail content may be programmatically monitored to identify if profanities are present. Where such facilities are in place, the procedures used will be disseminated on Parish Council intranets
- ◆ Networked servers: file ownership, file name, file size, file types, file dates (e.g. creation dates/modification date)
- ◆ Computer workstations: installed software: the type of software, time and date when it was installed
- ◆ Virus monitoring: All electronic traffic and files entering or stored on the Parish Council network are programmatically scanned for viruses and where viruses are found, the files are disinfected, deleted or quarantined

◆ Software transaction monitoring: Audit facilities operate on all of Parish Council's principal business systems logging system access and system transactions. For example the name of the user who updated a record, when this update occurred and what data items were changed

◆ Telephones and Faxes: All calls (incoming and outgoing) are logged for date, time, number called or calling, duration

◆ Voicemail: Numbers of calls stored, when stored and the data capacity of this storage

If employees have concerns about the information that may be disclosed through knowledge of any Internet addresses accessed, they should refrain from using such sites.

Reports based on the information described above may be produced and disclosed to the Parish Council.

In the context of this Code of Practice, all employees are able to request reports about themselves although Parish Council reserves the right to charge for such reports in line with guidance issued as part of the Data Protection Act.

12.2 Detailed Investigations

There are occasions when any files, e-mails, voicemails or software (including those marked as personal) stored on Parish Council-owned equipment may be subject to detailed inspection including an inspection of the content by properly trained members of employees. Employees undertaking approved investigations are not subject to the restrictions detailed in this CoP.

For this to happen, Parish Council approval must be obtained and such approval will be based upon evidence being presented to support the case for investigation. Evidence may derive from a number of sources including complaints made by other employees, members, or when a properly authorised request from a public authority or court order has been received.

The Parish Council authorising the request will do so in writing and will be expected to balance the benefits of investigation against any possible intrusion of privacy. In authorising the investigation, the Parish Council will take advice, where appropriate from relevant experts e.g. Clerk to the Council, the Head Steward and/or external experts. Specific written confirmation must be given for investigation into any file or message marked with a personal title/file name or stored in a personal folder. Investigations will be undertaken by the Clerk to the Council, the Head Steward or by an appropriate third party e.g. police officer.

Parish Council approval as described above is also required before the content of any telephone calls can be monitored or recorded.

If there are reasonable grounds for suspicion of criminal activity then Clerk to the Council will immediately inform the police and/or seek other legal advice.

13. Mobile Working and Wireless Facilities

In terms of computer equipment, these represent fast moving areas with rapidly changing technologies. Unless otherwise stated in this policy or in other official guidance issued to the employees, all the points made in this code of practice apply to those using Parish Council facilities to work in a mobile capacity.

Users of laptops, PDAs etc must contact the Clerk to the Council to discuss appropriate arrangements for ensuring that security software such as anti-virus software, system patches and/or personal firewalls are kept up-to-date. The Clerk to the Council will ensure that best practice and guidance is published.

Guidance on the local storage of data can be found at paragraph 9 of this appendix.

Where secure facilities have been provided for a Parish Council system or systems, employees must ensure they use these facilities.

Wireless facilities are subject to specific security risks. Wireless standards and procedures will be defined by computing partnership policy in line with Network Security Policies. Where wireless facilities enable access to internal Parish Council LANs, all connecting wireless equipment must comply with these standards. Where Parish Council has provided anonymous access to the Internet through wireless facilities, all users must comply with any specific instructions provided during the access procedure. Parish Council employees should be aware that the provisions of this code of practice apply. Parish Council devices must never be used to access or attempt to access wireless networks without appropriate authorisation even where these have been inadvertently detected by the device.

14. Incident Reporting

All employees must report actual or suspected security incidents or weaknesses to the Head Steward. For matters of a very sensitive nature or which may implicate these parties, employees should inform the Clerk to the Council.

If a employees encounters a virus on their system, they should contact the Head Steward and then stop using the workstation until the “all-clear” has been given. If employees are unsure if a file has been checked for viruses they must contact the Head Steward for advice before the file is opened or used.

15. Spam and Junk Mail

Employees should think carefully before responding to any junk, spam e-mail or SMS message etc even if this is to “unsubscribe” from a mailing list. Often the originators simply use the response as a way of confirming the legitimacy of the address, although others do act more ethically. Hard and fast rules cannot be provided and therefore, in general, employees are advised not to respond to “junk”, “fraud” or “spam” e-mails, fax messages or SMS messages.

The Parish Council will establish policies for automatically stopping incoming spam e-mail messages that will serve to protect Parish Council systems and employees from the worst excesses of e-mail spam; these policies will be available to employees. However, the policies are unlikely to be 100% effective and employees with particular concerns about messages they receive should contact the Head Steward. In addition, while every endeavour will be made to ensure that valid messages are let through, some may be stopped by mistake. If employees have concerns about any missing messages they should also contact the Head Steward.

Unfortunately, there is little that can be done to filter SMS or fax spam messages so the onus is on employees to act appropriately.

If an individual considers that the frequency of receipt of unwanted hard copy junk mail from a particular company is a nuisance, they should return the mail to the sender with a request to be removed from their distribution list.