



An Acceptable Use Policy

"Any organisation needs to inform its people about the type of behaviour it expects of those using technology in the workplace and about the consequences for abusing technology privileges".

What is your organisation's view on acceptable computer use?

There are no "black and white" answers, each area identified below requires your organisation to take a view on a scale of acceptability. The consequences of the view are raised later but the key areas for consideration are listed below.

- Forced recognition of security
- E-mail use
- Internet use
- Security of Data
- Backing up
- Mobile Phones
- General maintenance
- Security
- Viruses
- Spyware
- Security of the PC
- Care of the equipment
- Logging/monitoring

1. Forced recognition of security

If you will be monitoring the use of the computer, internet and/or e-mail it could be an invasion of privacy unless the computer user signs a statement or declaration that they are aware that you intend or might do so, e.g. "the management of reserves the right to monitor all computer use by users" This can be a part of the policy that each user signs or a separate sheet containing a summary of the rules for casual users.

2. E-mail use

Consider this as you would your policy regarding telephone use.

Key Questions

- Do you allow your employees to send personal messages using the organisation's e-mail address?
- Do you allow staff to access their private e-mails e.g. Hotmail, Yahoo — would you allow them to configure Outlook to read them?
- Does your anti-virus software scan all outgoing *and* incoming e-mails?
- Do you have a signature and/or disclaimer on the bottom of your outgoing messages?

- Do you have a maximum attachment size set?
- Do you limit what type of attachments you will allow in or out?
- What measures are you taking against Spam? Do you have internal and/or external anti-Spam filters?
- Are you staff aware of how to spam-proof messages?
- Do your staff know not to open “suspicious” e-mails?
- Do you have a central public facing e-mail, admin@..., office @... and each person then having their own individual address?
- Is your email address suitable— is it too long or it doesn't contain your organisation's name?
- Do you make sure that e-mail lists are not CC'd - do staff know how to set up BCC in a mailing list?

If you use mass emailing systems do you allow recipients to unsubscribe, keep databases up to date and follow CC and anti-spam best practice?

3. Internet use

Consider this as you would your policy on time keeping and being non-productive

Key Questions

- Do you allow your staff to explore the Internet for their personal use? If so for how long—breaks only?
- Is your Internet access limited or filtered—what type of sites are or are considered not “acceptable”? Who controls, monitors and updates this system — how much time are they given?
- How do you know what sites have been visited, by who and for how long? Do users share an id or login? Can individual use be identified?
- Do you allow downloads (e.g. MP3), streamed media (audio and video), installation of plug ins, software, Active X controls, etc?
- What is the position regarding Blogs, Wikis, Facebook, Twitter and other emerging interactive Web 2.0 technologies?
- Does your organisation have an “official” presence on such sites – who manages it? Are staff aware of their contractual obligations when contributing to such sites either officially or as a “private” individual?
- What is your position regarding “chat” and messenger systems, e.g. MSN, Skype, Yahoo, etc. Such systems can also be accessed by mobile telephones – do you allow staff to have such applications open?

4. Security of Data

This overlaps with many other areas of policy: Data Protection, care of the PC, passwords, backing up and virus procedure.

The focus of this section is what steps do you take to make sure that the data held on a PC is safe and secure from unauthorised access or use.



Key Questions

- Is all data password protected?
- Is file security invoked to make sure that no unauthorised access to data is allowed?
- Is data encrypted in transit?
- Are steps taken to make sure that the computer is free from viruses and spyware?
- Is data backed up regularly?
- Is hard copy kept in lockable and/or fire proof storage?
- Is your wireless network encrypted or has a mechanism to stop unauthorised access?
- Is your network protected by a firewall?
- Individual documents can also be password protected, however this raises issues relating to intellectual property and the ability to monitor the content of the hard drive.

5. Mobile Phones

Does your organisation provide staff with a mobile phone? If so do you have policies regarding its use?

- Personal calls/text - are you going to allow staff to make them using the company phone? If so when, how many and how long?
- Are you going to pay staff an allowance to cover use of their own phones? What are the tax implications?
- What is your view on video messaging, internet, video on demand and other emerging technologies? Regular reviews are essential.
- What is the policy regarding using a mobile phone whilst driving? Do you provide a hands free kit?
- What is the view regarding use of personal mobile phones during the working day? Do you limit the use to break times only and insist that the phone is turned off at all other times? What about texting, both receiving and sending?
- MSN messenger can also be a problem, what is the view regarding this and other mechanisms for online chat?

6. General Maintenance

Who is responsible for this — is a member of staff aware of these points and is adequately trained?

Check to see if the hard disc is getting full—delete all unwanted files regularly (Housekeep). Once a disc gets over 60% full you will notice it slowing down. “Defrag” the drive and remove temporary files at least once each month.

Windows updates need to be performed regularly.

7. Security

If you have broadband you must take “reasonable” steps to make sure that no-one can access your PC remotely. A FIREWALL blocks such access by unauthorised people or software.

If your PC has Windows XP (or newer) the operating system and has Service Pack 2 installed the Windows Firewall is adequate. We recommend Windows XP PRO, Windows Vista Business and/or Windows 7 PRO as “better” network security is built into the system.

Most modern Routers have built in Firewall—if you are unsure about yours contact your installer or the manufacturer.

If you have a router with a Firewall each PC does not need its own individual Firewall to protect it from outside interference.

If your PC has an older version of Windows (2000, 98, ME) and no Firewall at the Router then try Zone Alarm — however it is not free for VCO use. If you have a Dial Up or no Internet connection Firewall is not necessary.

All PCs must have password protected entry. Do you have a password policy?

It is a good idea to password protect your screen saver — never leave a PC logged on and unattended.

Apply security to key files on a network.

Keep all backup discs and media in locked drawers.

Be careful with CDs, Memory sticks and all other transporting media.
ALWAYS BACK UP YOUR DATA regularly

8. Viruses

A virus is a program that infects a PC by entering it through the Internet, E-mails, CDs, memory sticks, floppy discs and/or other networked PCs. Viruses can destroy data, disable a PC and spread to numerous other PC systems.

Most modern anti-virus software includes an anti-Spyware system. If you are unsure then check with the manufacturer, adding an additional anti-spyware product may slow the PC system down and cause clashes between the system components. Never combine two separate anti-virus systems, it will slow the PC system down and cause clashes – you will not have any more protection.

You **MUST** install anti-virus software even if your PC is not connected to the Internet.



You **MUST** also make sure that the anti-virus software is updated regularly (at least weekly) - new viruses come out daily.

Who checks to see if the anti-virus software is up to date?

What procedure do you have in the case of a virus infection? (Lock down, disconnect, scan) - Is this for all PCs on the network?

Is the incident and solution recorded?

Did you know that if a virus is spread via an e-mail sent on behalf of your organisation you can be held liable for damages as a result of the virus — make sure that your anti-virus scans all incoming and outgoing e-mails. If your computer starts to display “odd” behaviour (running very slowly, missing options, not responding to the mouse), re-boot it, make sure that your anti-virus software is up to date and perform a scan immediately.

DO NOT LEAVE the system to do a scan automatically — perform a manual scan at least once per week.

What is the policy on e-mail attachments, SPAM, unknown senders and/or opening suspect messages?

There are many good anti-virus products—not many are free to VCOs. Most anti-virus software relies on an Internet connection to update. There are anti-virus systems available on line (e.g. Housecall).

Other products include Norton, MacAfee, AVG, Panda — all at varying prices, most offer VCS discounts but none are free for use, except for *home* users.

9. Spyware

Spyware are pieces of computer code that, at best, slow your internet connection down and, at worst, can interfere with key PC functions (Malware). Spyware records your web browsing and “beams” it back to base through the Internet whilst you are surfing other sites. Some code can disable the start button, right hand mouse click and even blank the screen.

Spyware can only come from using the Internet. Some Spyware can activate or download a virus. Spyware can be called Malware, Ransomware or Greyware depending on its form and function.

Most anti-virus software has built in spyware protection. These are, however, large and resource intensive pieces of software that can slow your PC down considerably. Make sure that your PC has enough RAM and a powerful enough processor to cope with the demands of your chose anti-virus solution.

There are free on-line anti-virus products e.g. Trend Micro's Housecall.

Most commercial products are NOT free to VCOs (they are free for personal use only) e.g. AVG and Avast. By and large you get what you pay for in terms of IT, invest in a “good” system and it will afford a level of protection. Ask your IT supplier or other projects which products they use and what they are like.

What is the position regarding removable media? Are USB memory sticks scanned at *both* ends. Do you allow staff to use USB sticks to store data permanently, their own data or use on their personal PC? Is data held on memory sticks encrypted and/or password protected?

10. Security of the PC

This section covers the physical security, the integrity of the system (how fiddle proof it is) and the integrity of the data.

Key Questions

- What steps will you take to stop theft of the PC (locks, bolts, etc)?
- Have you got a record of the serial number and spec (an inventory)?
- Will all PCs have to have a password to access them?
- Does each user need to have “administrator” access to their PC i.e. do they need to be able to install and or delete software, change settings, etc?
- It is good practice that someone else knows the administrator password for each PC. Consider a password book.
- Do you allow users to store their own personal information on the PC, if so what, where and how is it transported to and from the PC, what about intellectual property rights? Who is responsible for backing up?
- Will each user have a unique log on (user id) to their PC?
- Will Internet access be password protected and/or filtered?
- Do you allow your users to alter the background on their desktop—if so what images are and are not acceptable?
- Is “housekeeping” performed regularly?
- Are other maintenance tasks e.g. “defragging” performed regularly?

11. Care of Equipment

Many of the problems associated with IT are a result of poor maintenance or user intervention.

Key Questions

- Who is responsible for the equipment?
- Will it be cleaned regularly?
- If staff are to clean their own PC systems do they know what to use to clean various parts of the system? E.g. damp cloth, anti-static wipes, etc — are these in stock?
- Will it be checked regularly? (PAT tested)
- Are other preventative measures in place — surge protectors, UPS?



northern rock foundation

Circuit Riders



- Is the PC system and all its parts securely on a desk or table?
- Do you allow staff to connect their own equipment (e.g. PDAs, iPods, headphones) to your PC systems? If so who is responsible any for damage to, or malfunction of, the PC or attached device?
- Do you allow staff do perform work tasks on their personal PC systems? If so who holds intellectual rights?
- What is the view on data security (viruses and encryption), access to and transfer - Do you allow systems to "sync"?
- Do staff work from home and/or remotely - what are the arrangements and procedures relating to data transfer and network access?

12. Logging and Monitoring Use

This can be done by something as simple as a sign up list or complex server software—which can be expensive.

Internet use can become a problem if individuals spend time booking holidays, shop on e-bay or look at unsuitable material. Use of other devices such as webcams and chat rooms can also prove to be an issue.

Free (e.g. OpenDNS) or low cost software (e.g. Netnanny) can provide evidence of misuse and keep unproductive use to a minimum. These, as do all monitoring systems, have a training and management overhead.

Under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 it is deemed "lawful business practice" to monitor communications (including telephone and e-mail) to "determine whether they are communications relevant to the system controller's business".

This does not cover monitoring which Internet sites users have visited or attempted to visit. A forced recognition of security is still required in this case and also to monitor what is stored in the PC.

Disciplinary procedures may have to be amended as a result of changes in IT policy.