COMPUTER USE POLICY

Policy Name:	Computer Use Policy
Owner:	IT DCEO
Review Dates:	June 2015 July 2017
Review Process:	Annual
Related Documents:	Data Protection Policy Retention Policy Social Media Policy

Please note our current IT provider is: Redpalm.
The manager in charge of IT is: David Duckitt, Services Manager

This policy covers the following:

1. INTRODUCTION

Misuse of computers by employees or volunteers of The Church Army can have large repercussions on the organisation, not only because of the potentially destructive consequences on our IT systems, but also as a result the potential legal liability the organisation may have for the unlawful actions of its employees, and due to the potential for discrimination claims due to inappropriate content being viewed or circulated at work. This being the case it is essential that all staff understand and follow the policies described below.

Please note that email and internet use (and indeed any other use of the Church Army computer systems) is monitored and logged to ensure compliance with the policies below or for any other reason. Be aware therefore that material of a strictly private or personal nature may be compromised if sent or received over organisation systems. Your use of the organisation's systems indicates consent to such monitoring and no further notice or consent by users to such monitoring is required.

Failure to follow the policies below may, depending on the importance of the violation, constitute a disciplinary offence, which could lead to dismissal. These policies are so important that any violation could constitute gross misconduct and justify dismissal without notice or payment in lieu of notice.

2. COMPUTER SECURITY AND VIRUS PROTECTION

2.1. User ID and Password

All employees with be given a computer ID at the start of their employment with Church Army and will be asked to create a password. Your computer ID password should be as secure as possible and must never be the same as your user ID or include any part of the ID. You are responsible for all activity performed with your User ID and therefore should never be given to someone else to use or be written down. Attempting to gain access to any system resources or to another employee's file for which you are not authorised is strictly forbidden.

If you forget your password, you must contact the IT department who will arrange for a new password to be set up. You should ensure that you set a new password for yourself immediately after this has happened.

2.2. Locking your screen

If you are going to be away from your desk for a few minutes you should lock your computer by pressing Ctrl-Alt-Del. If you're leaving your work area for an extended period, then your computer should be logged off and shut down.

2.3. Laptops

Laptops are full of exclusive organisation information and must be handled with caution. Do not leave laptops unattended outside of organisation premises. If a laptop is lost stolen it is essential to report the loss *immediately* to the Services Manager based in Sheffield so that unauthorised users cannot gain access to the system. Having a laptop lost or stolen is of course not a violation of the organisation's computer policy, but failing to report the loss immediately is.

Laptop security extends to hard-disk encryption. If your laptop has the capability to be encrypted then encryption of all organisation-related files and folders on the hard drive should be activated, so that loss or theft of the laptop will not compromise organisation information. If you carry a laptop contact the IT staff for further guidance as to how to implement encryption in accordance with this policy.

Software may only be loaded onto a user's computer with the approval of IT. Do not attempt to load personal software onto your computer without their assent because of the conflicts such software may create with the organisation's systems

Floppy disks, CD-ROMs or other removable media received from third parties should not be loaded onto your computer without the approval of the IT staff who will virus-scan any such media prior to loading onto the system. (Information on using removable, portable memory and mobile devices is set out later in the policy).

3. COMPUTER PROPERTY

All computers, laptops, printers, phones and other digital technology given to an employee by Church Army for the purpose of work remain the property of Church Army and at the termination of your employment will be expected to be returned to Church Army.

Limited personal use of computers is permitted provided it:
is not illegal;
does not adversely affect other users;
does not interfere with work or studies;
or in any other way breach the conditions of the computer use policy.

4. EMAIL AND INTERNET

Church Army encourages its employees to use email and the internet at work where this can save time and expense. However, it requires that employees follow the rules below. It is a term of each employee's contract that he/she complies with these rules, and any serious breach could lead to dismissal. Any employee who is unsure about whether something he/she proposes to do might breach this email and internet policy should seek advice from his/her manager.

Although the organisation encourages the use of email and the internet where appropriate, their use entails some risks. For example, employees must take care not to introduce viruses on to the system and must take proper account of the security advice below. Employees must also ensure that they do not send libellous statements in emails as the organisation could be liable for damages.

4.1. Use of email

Contents of emails

Emails that employees intend to send should be checked carefully. Email should be treated like any other form of written communication and, as such, what is normally regarded as unacceptable in a letter is equally unacceptable in an email communication.

The use of email to send or forward messages which are defamatory, obscene or otherwise inappropriate will be treated as misconduct under the appropriate disciplinary procedure. In serious cases this could be regarded as gross misconduct and lead to dismissal.

Equally, if an employee receives an obscene or defamatory email, whether unwittingly or otherwise and from whatever source, he/she should not forward it to any other address.

Email Signatures

Employees should ensure that they use the correct Church Army Signature on any emails that they send. Details of what this should be are available from the Communications Team.

Attachments

Employees should not attach any files that may contain a virus to emails, as the organisation could be liable to the recipient for loss suffered. The organisation has virus-checking in place but, if in doubt, employees should check with the IT department.

Employees should exercise extreme care when receiving emails with attachments from third parties, particularly unidentified third parties, as these may contain viruses.

4.2. **Personal use of email**

Although the email system is primarily for business use, the organisation understands that employees may on occasion need to send or receive personal emails using their work address. When sending personal emails, employees should show the same care as when sending work-related emails. These should not be in conjunction with any other business you may be involved with.

4.3. **Monitoring of email**

Church Army reserves the right to monitor employees' emails, but will endeavour to inform an affected employee when this is to happen and the reasons for it. The organisation considers the following to be valid reasons for checking an employee's email:

- If the employee is absent for any reason and communications must be checked for the smooth running of the business to continue.
- If the organisation suspects that the employee has been viewing or sending offensive or illegal material, such as material containing racist terminology or nudity (although the organisation understands that it is possible for employees inadvertently to receive such material and they will have the opportunity to explain if this is the case).
- If the organisation suspects that an employee has been using the email system to send and receive an excessive number of personal communications.
- If the organisation suspects that the employee is sending or receiving emails that are detrimental to the organisation.

When monitoring emails, the organisation will, save in exceptional circumstances, confine itself to looking at the address and heading of the emails. The organisation will avoid, where possible, opening emails clearly marked as private or personal.

The organisation reserves the right to retain information that it has gathered on employees' use of email for a period of one year.

4.4. Access to Emails

If access to emails is required, the following protocol has been agreed:

- If access is needed to an inbox, the line manager, or HR manager, needs to approach a member of SLT for authorisation.
- If access is required to the inbox of a member of SLT, that needs to be agreed by the Chief Executive and a member of the Board.
- If access is required to the CEO's inbox, that needs to be agreed by the Chair and one other member of the Board.

4.5. Use of internet

Sensible internet use

Where employees are allowed access to the internet at work they are expected to use it sensibly and in such a manner that it does not interfere with the efficient running of the organisation.

Employees may be called upon to justify the amount of time they have spent on the internet or the sites that they have visited.

The organisation encourages employees to become familiar with the internet and does not currently impose any time limitation on work-related internet use. It trusts employees not to abuse the latitude given to them, but if this trust is abused it reserves the right to alter the policy in this respect.

Removing internet access

Church Army reserves the right to deny internet access to any employee at work, although in such a case it will endeavour to give reasons for doing so.

Licences and contracts

Some websites require the organisation to enter into licence or contract terms. The terms should be printed off and sent for approval in advance or emailed to the legal department before an employee agrees to them on the organisation's behalf. In most cases, there will be no objection to the terms and it is recognised that the free information provided by the website in question may save the organisation money. Employees should, however, always consider whether the information is from a reputable source and is likely to be accurate and kept up to date, as most such contract terms will exclude liability for accuracy of free information.

Downloading files and software

Employees should download files on to only those PCs with virus checking software and should check how long the download will take. If there is any uncertainty as to whether the software is virus-free or whether the time the download will take is reasonable, the relevant line manager and the organisation's IT department should be consulted.

4.6. Monitoring of internet access at work

Church Army reserves the right to monitor employees' internet usage, but will endeavour to inform an affected employee when this is to happen and the reasons for it. The organisation considers the following to be valid reasons for checking an employee's internet usage:

- If the organisation suspects that the employee has been viewing offensive or illegal material, such as material containing racist terminology or nudity (although the organisation understands that it is possible for employees inadvertently to view such material and they will have the opportunity to explain if this is the case).
- If the organisation suspects that the employee has been spending an excessive amount of time viewing websites that are not work related.

The organisation reserves the right to retain information that it has gathered on employees' use of the internet for a period of one year.

4.7. Social Media

Church Army operates a Social Media policy which details more specifically our expectations in the use of social media whilst at or for work purposes. All employees are to adhere to this policy.

5. REMOTE WORKING

Church Army provides a secure network infrastructure to give employees the flexibility to work remotely. However, it is the employee's responsibility to take the necessary steps to maintain a physically secure and virus-controlled workstation environment. It is also the responsibility of the employee to ensure that the appropriate access controls to Company information are in place.

- All requests for remote access must be approved by your Line Manager.
- All remote access users must only use equipment and software that is compliant with Church Army Security Standards.
- Anti-virus software, security firewalls, or other security software/hardware must not be disabled at any time.
- Note that the IT Department retains the right to inspect any computer system that is connected to its network.

6. STORAGE OF COMPUTER FILES

- The IT Department is not responsible for any data saved on your Local Hard Disk (C or D Drive) which includes saving any files on your Desktop.
- *Laptop users must make manual backups (Write to a CD) for any files they wish to use on their Local Drive (C: Drive) which also includes any Archived email (Personal Folders) in Microsoft Outlook. Where these contain work files these need to be security protected*
- Our Business Constituency Plan requires that all your work related files have to be saved on your network drives (P and G).
- The P drive is the space set aside for your own personal work related files. No other user has access to these files.
- The G drive is the shared drive in your department. Users in your department can view the files saved here.
- No Personal Music / Videos / Pictures are allowed to be stored on the server.

7. ACCESS TO FILES

At the start of your employment, your line manager will ensure that you have the correct access to the relevant files you need on the server.

If for may reason you need to access different files, you must seek permission from your line manager first to then ask the IT department. The IT department is forbidden to provide you access to a file without authorisation from your manager first.

8. USE OF DATA STICKS AND OTHER PORTABLE MEMORY AND MOBILE DEVICES

The policy provides guidance to staff on the secure use of mobile technology for carrying confidential, sensitive and Person Identifiable Data (PID).

USB memory sticks, external hard drives, mobiles/tablets and CD/DVDs have become increasingly popular because of their small physical size and large storage capacity. This has made them very convenient devices for carrying files from one place to another. However, these very features have introduced new information security risks:

- Potential breach of confidentiality – if the mobile device is lost or stolen.
- Physical loss – being so physically small the memory stick can be easily lost.
- Access to information and Emails through Mobiles and Tablets
- Virus transmission – memory sticks can introduce viruses onto a computer network.

USB memory sticks may be used for non-confidential information but should not be used in any CA machine which does not have up to date antivirus software.

8.1. Reducing the risk of losing information

There are several main ways of preventing the loss of information:

- Avoid physically carrying such information
- Encrypting confidential, sensitive & Person Identifiable Data
- Setting secure access passwords or key codes for Mobiles/Tablets

8.2. Data Avoidance

Confidential, Sensitive and Person Identifiable Data must not be stored or carried on non encrypted memory sticks. Staff should use other secure methods for carrying such information:

- Storing information in relevant secure departmental folders on the shared ‘G’ drive. Your departments ‘G’ drive folder can be accessed on any CA networked computer.
- Encrypted CA issued laptop computers.

8.3. Encryption

Where a need has been identified and agreed with a manager that an encrypted memory stick is required to carry confidential, sensitive or PID, a request must be made via the ICT helpdesk for an approved encrypted device.

An encrypted memory stick allows information to be stored but renders the information undecipherable unless the correct password is entered.

Encrypted memory sticks will be issued to specifically named members of staff for their professional use. They must not share the device with other persons. They must not share or disclose the password to other persons.

NB

Confidential, sensitive or PID carried on encrypted memory sticks must not under any circumstance be placed on non CA issued computers.