



Responsible Trustee	Date policy produced	Name of Policy Writer	Frequency of Review	Date reviewed on / by whom	
	31 May 2016	Tony Wilkes	Every 3 years	John Milroy/ Tony Wilkes	5 November 2018

## Cambray IT Policy

### Introduction

This policy is designed to provide procedures and guidance for the maintenance and security of the computer equipment owned by and used by staff and volunteers at Cambray Baptist Church (CBC).

### General

CBC has invested considerable time, money, and people resources into providing computer hardware, software, and networking to equip the Staff and volunteers to perform their varied functions. All computer systems and their content are the property of CBC and are provided to enable users, whether employed or voluntary, to carry out their duties.

To ensure that its systems are used for ministry purposes, are secure and in compliance with copyright laws, CBC reserves the right to monitor all systems and their use. However, employment at CBC does not guarantee access to a computer or related resources.

It is the responsibility of employees or volunteers to take reasonable efforts to safeguard the valuable equipment and data provided.

Staff members and volunteers are representatives of the CBC. Any use of CBC computer equipment is an extension of that representation. With access to e-mail and the Internet, CBC can be represented worldwide, almost instantly.

CBC's policies are intended to protect both the Church and the computer user. Violation of policies may have serious consequences which could include grounds for dismissal, legal or civil action.

The policies are detailed below. Failure of individuals to read and understand the policies or ignorance of their existence does not excuse violation.

### Appropriate Use

Computers, like most other things, are tools that can be abused. When connected to the Internet, as CBC's computers are, abuse can be very counter-productive, embarrassing to the Church, or even illegal.

- Jokes and feel good messages should not be forwarded on CBC computers. Remember, many of these emails are not factual and have been circulating the internet for years. These messages are a waste of resources, and time.
- In general, limit forwarding of non-church e-mail, except for members' prayer requests.
- All CBC users are reminded to check that any copyright limitations are carefully observed. Images, quotations from external documents and the like are often copyright and should not be used by CBC unless specific permission has been obtained in writing.
- The music and related words that are used in church services are almost always covered by copyright. CBC have a licence from Christian Copyright Licensing International (CCLI) which permits us to use a very wide range of music for church services. However, it should be noted that not all hymns and songs are covered by this licence and so those involved in organising services should be very careful to only use licensed material. If in doubt, ask!

## Hardware

Adding hardware to, reconfiguring hardware on, or removing hardware from CBC computers is prohibited regardless of who pays for it. If you feel that the hardware needs attention or is not adequate, please request assistance in writing from the Church Manager. This will ensure that all requests are handled centrally

- Hardware is to be moved only by the Church Manager unless prior consent has been given.
- The use of USB flash drives is permitted but special care must be taken to ensure that viruses are not unwittingly introduced to the system. It is strongly recommended that any such drive has been scanned for viruses prior to use.
- All users must be approved by the Church Manager and have signed and agreed to the computer policies as laid out in this document.
- Personal Computers, laptops, PDA's, phones, etc. are not allowed on the network without authorisation from the Church Manager
- Employee access to a computer system does not grant access to family members or friends, unless they have been approved for computer use by the Church Manager.
- Passwords are not used to protect a user's privacy interest or to imply an expectation of privacy, but for the security of the computer system and network. Passwords must be at least 6 characters with a combination of numbers and letters. Passwords are to be changed periodically to maintain security. Passwords should not be given to anyone at CBC except the Church Manager. Passwords should not be posted or written in your desk or work area. If someone needs access and isn't set up, notify the Church Manager who will set up a user id.
- Sharing of user names and passwords should be the exception rather than the rule. An example of where this practice is acceptable is on the video desk which is used by a number of individuals and where access to the system is intentionally limited. Any other sharing for an urgent need must be sanctioned by the Church Manager and once the need has been satisfied, the password will be changed.
- If a user leaves their computer unattended, it should be locked to prevent unauthorised access. To lock the computer, press control, alt, delete and then click on **Lock computer**. Depending upon the computer keyboard in use, the Windows key + the letter L may also be used.
- Computers should always be switched off before leaving the church premises or if you will be away for an extended period of time.

## Computer Configuration

- Computer settings and configurations must only be modified or adjusted by the Church Manager. No-one else is permitted to change the configuration of any CBC computer.
- Acceptable changes to any CBC computer include screen colours, wallpaper and desktop shortcuts.
- Unacceptable changes to any CBC computer include such things as adding a screen saver installing shareware or any other unauthorised software, etc.
- If you have questions concerning configuration, settings or installed software, please direct those to the Church Manager.
- The hard drives are not filing cabinets and need to be tidied up periodically.
- Any additional hardware needs must be submitted to the Church Manager in writing for approval, this includes printers, handheld devices, mice, etc.

## Repairs and Maintenance of Computers

- If a problem arises with a computer system or device, refer to the FAQ's and reboot to see if it resolves the problem. The user is responsible for reporting problems to the Church Manager. Please don't complain about issues that haven't been reported. If you share a computer, don't assume that any other user has reported the issue. Problems can only be fixed once they have been reported.
- If a problem persists, please report back to the Church Manager with as much detail as possible.

- Not all repairs and upgrades can be handled the same day or hour that they are reported. The Church Manager will assess the situation and determine the course of action.
- The Church Manager, IT designated individuals, or approved vendors are the ONLY ones that are allowed to service any CBC computer equipment. Under no circumstances should computer cases be opened, computer cards installed or removed, cables removed or replaced, or any other equipment from within or attached to any computer be connected, disconnected or modified. If there is a problem, the Church Manager should be contacted.

## Software

- All authorised, approved and licensed software has already been pre-loaded onto CBC computers.
- Users must not load any additional software onto any CBC computer. This includes screensavers, shareware programs, personal copies of anything (unless approved in writing), utilities, drivers, web browsers etc.
- If additional software is required for your ministry area, please obtain permission from the Church Manager. Be prepared to provide a valid reason that has to do with your productivity or the needs of your role within CBC. Games and online viewers are not allowed.
- All Software and licenses will be stored in one central location.
- The church maintains one centralised database for the church member records. This data is supported by the ChurchBuilder software which is administered by CBC webmasters. Backups of this data are maintained by Concordant Ltd who are the suppliers of the software. No other databases will be supported. Storage of personal data will be in accordance with the requirements of the Data Protection Act as described in the CBC **Data Protection Policy** and in the Baptist Union document **L13\_DataProtection**.
- Unauthorised software may be removed without warning. If a user installs software that causes a problem with the normal use of the computer, the Church Manager will not treat this as an emergency. Restoration of normal operation will take place when time is available and it is very possible that not all the previous functionality will ever be restored. Any items stored on the local disk drive, including data, may be lost forever.
- Non-standard software requires a disproportionate amount of time to install and support. Users are not permitted under any circumstances to load programs onto computers at CBC, or supplied by CBC, without prior permission from the Church Manager.
- We have installed virus protection on many levels. All e-mail messages, downloads, and files are scanned when received. If one of these contains a virus, the program first attempts to remove the virus from the item. If successful, the item is delivered into the recipient's mailbox and browser. If it cannot be extracted, the item is placed in quarantine where it cannot be accessed and the Church Manager is notified.
- Common sense should prevail when using email as it is provided primarily for church business and ministry purposes.
- Attachments to an email message could contain a virus that would harm your computer, harm everyone else on the CBC network or send itself automatically to everyone in your address book. Our most important line of defence against a computer virus is users who follow these rules. These instructions must be followed even if the e-mail is from a trusted source. These instructions must be followed even if you think you can see the full name of the attachment. Be suspicious even if you know and trust the sender. If you receive a warning that an attached file contains a macro, **disable** the macro.
- If you receive email telling you to delete certain files, forward the message to the network administrator, but **do not delete** anything, even if it is a reliable source until it can be confirmed as legitimate. If you receive emails about new viruses, forward to the Church Manager to validate and not the whole staff.
- All emails, sent items, deleted items should be archived periodically and at least every three months. This preserves disk space and keeps the email running smoothly.

## Database and List Management

- Your computer and all the software and data contained on it or on the network servers are the property of CBC. This is true whether created by you or someone else. Except in circumstances where specific Intellectual Property Rights (IPR) exists, the data files on the network also belong to CBC. You should use caution when creating files that reside either on your computer or on the network that are of a highly personal nature. CBC does not guarantee privacy or continued access to any material created or placed on the network or your hard drive.
- In general, security has been established to protect files from unauthorised access, modification, or accidental deletion. However, CBC reserves the right to inspect and/or open any data files which reside on the network or local hard drives at any time.
- The user is responsible for the backups of any data stored on the local drive, desktop, laptop or other computer device.
- Network backups, which include network drives, database information and email are the responsibility of the Church Manager.
- All membership data is maintained in a centralised database to maintain the integrity of the data and should not be kept outside of this database, this includes emails, names, addresses, phones, etc. This data should be considered confidential and not given out except by authorisation for a specific ministry area. This authorisation should be given by the minister in charge of the specific area or the Church Manager.

## Physical Security

- Employees are expected to take reasonable measures to protect computers, data, and the network, from unauthorised access. For desktop users, this means properly guarding passwords, locking doors and computers as appropriate, and being aware of non-Staff member using Church resources (computers).
- Notebook users need to be much more proactive about security. (Approximately 1 in 14 notebook computers are stolen nationwide. Notebooks must never be left in an unattended area. This includes leaving systems on a desk overnight, even if the office is locked. Leaving a system on a desk, even during the day, when it is not certain that other Staff members are nearby is equally risky. Likewise, they should never be checked as baggage nor left visible in an unattended car. Notebook computers are for employee use only and not for family and friends.

## Network Security

The Church Manager has taken every precaution to protect our network and its data from purposeful or accidental damage or destruction. The key element in that security model is your login name and password. It is recommended that this password be changed frequently and be a combination of letters and numbers. Please avoid using family, friends or pets' names as a password. Each login name/password combination gives different and specific rights and permissions to access network resources to each user (e.g. you have different access rights than another Staff member might). Therefore, sharing your login name or password with anyone (including Staff members) is strictly prohibited. Allowing someone to use your computer logged on as you (e.g. you let them sit down at your computer without you logging off) is also prohibited.

If an authorised user needs to use your computer, you must log off and let them log on as themselves. If an unauthorised user (one who does not have their own login name and password) wishes to use your computer or the network, you must send an email request to the Church Manager asking that an account be created for that person. This request should be made in advance. There are no exceptions to this requirement including family and friends. This includes notebooks that are often used at home. The equipment and its contents continue to be a part of our network regardless of where they are used.

## **The Internet**

- Access to the Internet has been given to you primarily to assist in your work.
- Surfing the web for personal reasons must be avoided at all times
- Viewing or downloading of materials or Internet sites that would not be glorifying to God or edifying to others is strictly prohibited. A definition of unacceptable site content can be provided upon request, but most of you will know this instinctively.
- Downloading and then installing programs from the Internet onto your CBC computer is strictly prohibited. This includes games, "trial" versions of software, fonts, sounds, graphics, shareware programs, screensavers, etc.
- Chat areas of the Internet are not a good use of our time and are therefore, prohibited unless a valid reason can be given to use them (there won't be many).
- CBC reserves the right to audit Internet use, including websites visited, as an accountability tool for those Staff that might be tempted to get into areas they shouldn't.

## **End of Employment**

Upon conclusion of employment at CBC, login rights and CBC e-mail address will be deactivated and personal directories will be removed from the network. Files cannot be removed from the network without the express approval of the Church Manager and the leadership of the Church.

## **Resources and Training**

Training will be offered as needed. Please notify the Church Manager for any training that you need.

# 1 Employee Statement of Acknowledgment

This is to acknowledge that I have received a copy of the Cambray Baptist Church IT Policy manual. I understand that it provides guidelines and summary information about our Ministry's information systems policies, procedures, and rules of conduct. I acknowledge specifically that all email, computer and communications equipment, software, networks, and systems, Internet and other online access and/or email accounts, and all other computer and communications mechanisms (collectively referred to in this Handbook as "computer systems" or "systems"), are the property of CBC and are provided to enable me solely to carry out my duties for CBC and for its ministry purposes, and that all email messages and other content I may create in my service to CBC are and shall remain the exclusive property of CBC. I also understand that it is my responsibility to read, understand, become familiar with and comply with the standards that have been established in this Manual. I further understand that CBC reserves the right to modify, supplement, rescind, or revise any provision or policy from time to time, with or without notice, as it deems necessary or appropriate. I further understand and agree that any violation of CBC's policies or procedures may lead to disciplinary action, up to and including termination of my employment with CBC.

---

Employee or Volunteer's Name (Please Print)

---

Employee or Volunteer's Signature

---

Date