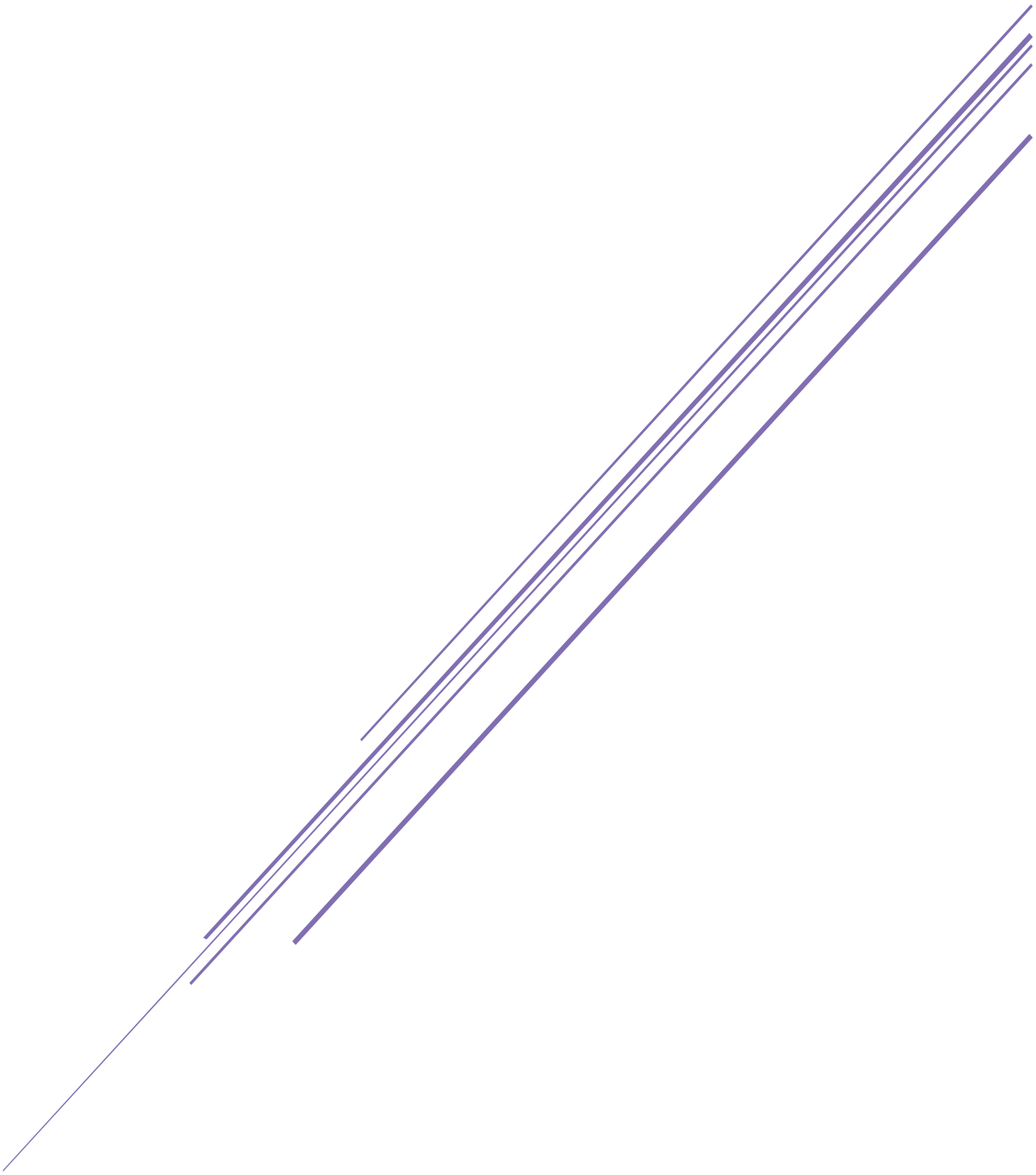
INFORMATION TECHNOLOGY POLICY

Holy Trinity Church

2 Upper King Street
LE1 6XE



Nov 2019

Review History

Prepared by: Stephen Gorton, James Banks, Kevin Maloney

Reviewed by:

Approved by _____ on _____

Next Review due:

Contents

1 Introduction

The widespread usage of Information Technology throughout day-to-day life continues to spread. Although data protection remains a significant part of UK law, we must also consider how IT devices are used on a daily basis and how they can impact upon Holy Trinity Church.

For the purposes of clarity, **data** means information which –

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,

(b) is recorded with the intention that it should be processed by means of such equipment,

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or

(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

1.1 Who this policy applies to

This policy provides clear guidance on the responsibilities of Holy Trinity Church, its staff and key volunteers. It defines guidance for acceptable use, security and data transfer. Anyone who uses any of the IT facilities provided by Holy Trinity Church should be aware of and have received a copy of this policy.

It further includes guidance for social media usage in particular for staff.

Deliberately or recklessly ignoring the guidance in this Policy including divulging or misusing confidential information will result in disciplinary action.

1.2 Acceptance of this policy

By using any of the Holy Trinity IT systems users accept that they will abide by this policy. Before using any system users should be familiar with this document.

1.3 Support Team

For any clarification on this policy or for all IT enquiries and support your contacts are as follows:

James Banks (IT Officer)
jbanks@htl.church
07772 154 719

Stephen Gorton (IT Director & Data Protection Officer)
sgorton@htl.church
07779 335 736

1.4 New Users & Key Summary

All new users to the Holy Trinity IT systems will be given a basic induction on the safe and correct use of the systems depending on their previous experience and knowledge. As a minimum the following will be highlighted to them and a copy of this policy given to them:

- Usernames & Passwords are to be kept safe and not written down or shared with anyone. Passwords should not be easy for someone to guess.
- All IT usage is monitored this includes internet and emails.
- Holy Trinity devices and IT systems should only be used for church business.
- All devices used for Holy Trinity must confirm to the minimum standards set out by this policy.
- Any devices (including personal) that have been used for Holy Trinity and are stolen must be reported as soon as it is noticed and without delay, to the IT support contacts at the start of this document.
- All devices and security software must be kept up to date.
- Where possible memory sticks and external drives should not be used, in the rare event memory sticks are used, they must be encrypted.
- Only connect to reputable Wi-Fi networks or those operated by Holy Trinity.

2 IT Systems & Device Usage Policy

2.1 Passwords

2.1.1 Accounts must always be password-protected, unless there is any exceptional circumstance in which it is not possible for this to happen. This can only be confirmed by the IT Director.

2.1.2 Passwords should be easy to remember and hard for somebody else to guess. First-time passwords (e.g. when a new user is registered) are temporary and must be changed as soon as possible by the user.

Some systems will have specific complexity requirements for passwords that are enforced automatically such as Uppercase or Lowercase letters. A good principle to follow when creating a password is 'three random words', for example 'coffeetrainfish'. This fulfils the requirement of being easy to remember but it is hard for somebody else to guess. Passwords may also need to contain a number or an upper case letter so each of the words could start with a capital and some of the letters could be substituted with numbers. Avoid using the same passwords for your home and work accounts.

2.1.3 Passwords should be changed only when there is reason to believe a password has been compromised. In this event the password will be changed immediately.

2.1.4 Usernames & Passwords must not be shared with those who have no permission to use them; this includes the staff Wi-Fi network keys.

Holy Trinity recognises that it can be difficult for users to remember lots of different passwords and so recommends the use of a password manager app on your computer or mobile device. This allows you to store passwords securely in a way that is hard for hackers to compromise. Do not write passwords down in notebooks or on paper near a device. Passwords should not be stored in standard files on a device such as a word documents. For further information and advice on password managers please speak to an IT administrator, detailed at the start of this document.

2.2 Acceptable Use

Holy Trinity provides staff access to the vast information resources of the Internet with the intention of increasing productivity and enhancing church-related communication. While this access has the potential for staff to do their jobs faster or smarter, there is justifiable concern that it can also be misused. Such misuse can waste time, potentially violate laws, ordinances or other Holy Trinity policies, garner negative publicity for the church and potentially expose it to significant legal liabilities. This Acceptable Use Policy, which applies to all employees and computer users, is designed to facilitate understanding of the expectations for the use of these resources.

2.2.1 Internet access, provided by Holy Trinity, not including any publically available Wi-fi service, is primarily for church-related purposes including communicating with church members and colleagues, researching relevant topics and obtaining useful business information.

2.2.2 All existing laws and Holy Trinity policies apply to a user's) conduct on the Internet, especially those that deal with intellectual property protection, privacy, misuse of Holy Trinity resources, sexual harassment, information and data security, and confidentiality.

The best way to determine if use of the Internet is appropriate is to ask, "If I were doing this same activity in some other way (e.g. telephone, library, in person, by hand) would this activity be appropriate?" The two key tenants to this usage policy are:

1. *Do not do anything with Holy Trinity Internet access resources that would otherwise be considered illegal, grossly inappropriate, or offensive to the established value system expressed by Holy Trinity as a Christian, charitable organization. Viewing or downloading erotica, playing games, sending non-Holy Trinity related mass mailings, and running a private business are obvious examples.*
2. *Do not waste Holy Trinity's resources. There are plenty of fascinating sites to explore, but Holy Trinity time should be spent conducting Holy Trinity business. Church employees may use their Internet facilities for non-business research or browsing during lunch and outside of work hours, provided that all other usage policies are adhered to.*

2.2.3 Employees and volunteers will not use Holy Trinity's Internet access facility to visit sites which are:

- Illegal under current law;
- Defamatory, threatening or intimidatory or which could be classed as harassment;
- Contain obscene, profane or abusive language;
- Contain pornographic material whether in writing, pictures, films or video clips;
- Contain offensive material regarding sex, race, religion or any disability or sexual orientation;
- Infringe third party rights or otherwise unlawful.

2.2.4 The following explicit prohibitions apply to computer and Internet usage:

- Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about any individual's race, age, disability, religion, national origin, physical attributes, or sexual preferences shall be transmitted.
- No abusive, profane, or offensive language is to be transmitted through the Church's e-mail or internet system.
- Further, electronic media may not be used for any purpose that is illegal, against church policy, or contrary to the Church's best interests. Solicitation of non-church business, or any use of the Church e-mail or internet for personal gain is prohibited.
- The display of any kind of obscene image or document on any Holy Trinity computing resource may be a violation of existing Holy Trinity policy on sexual harassment and is prohibited. In addition, obscene material may not be archived, stored, distributed, edited, or recorded using Holy Trinity network, printing, or computing resources. A user, who finds him or herself connected accidentally to a site that contains sexually explicit or offensive material, must disconnect from that site immediately and report the accidental connection to the IT Director.
- No user may use Holy Trinity's facilities to deliberately propagate any virus, worm, Trojan horse, trapdoor, or back-door program code or knowingly disable or overload any computer system, network, or to circumvent any system intended to protect the privacy or security of another user.
- Holy Trinity's Internet facilities and computing resources must not be used to knowingly violate the laws and regulations of the United Kingdom or any other nation, or the laws and regulations of any state, city, province or local jurisdiction in any material way.
- You must not download executable files, including freeware or shareware, from the internet unless authorised to do so. Where necessary, permission must be obtained in writing from Information Security.
- You must not publish executable files, including freeware or shareware, to the internet.

- The definition of executable files are files created in a format that the computer can directly execute or run. These files can harbour viruses or other harmful malware and can make unauthorised changes to your computer.

2.2.5 Holy Trinity reserves the right to block access to any site.

2.2.6 Holy Trinity will take reasonable steps to block any site that we deem inappropriate.

Holy Trinity cannot guarantee that all inappropriate content will be blocked. If you gain access to a site that you deem inappropriate, close your web browser immediately.

2.2.7 The viewing of Live TV by anyone on any device connected to Holy Trinity's Internet access facility must be covered by the user's own licence(s) where required. Holy Trinity is not responsible for this.

Live TV means any programme you watch or record as its being shown on TV or live on an online TV service. An online TV service is any streaming or smart TV service, website or app that lets you watch live TV over the internet. This includes services like All 4, Sky Go, Virgin Media, Now TV, BT TV, Apple TV, YouTube, Amazon Instant Video and ITV Hub.

2.3 Privacy

2.3.1 Holy Trinity may log details of Internet activity, including sites visited, etc., in order to ensure compliance with this policy.

2.4 Software

2.4.1 Purchased software and software documentation may be copied only as specified by the vendor. No versions of any purchased software are permitted beyond the number the church has purchased.

2.4.2 Personnel, Members and Friends of the Church may not purchase or write their own software for use in the Church without authorization. The downloading of any unauthorized software to church-owned hardware is also not permitted.

2.4.3 Freeware, shareware and commercial software from the Internet may be subject to computer viruses, may not work properly, or may be subject to copyright infringement laws. Users may download only software with direct business use with permission of the IT Director, and must arrange to have such software properly licensed and registered.

2.4.4 Users must not use Holy Trinity Internet facilities to download entertainment software or games, or to play games against opponents over the Internet. No user may use Holy Trinity facilities knowingly to download or distribute pirated software or data. Any software or files downloaded via the Internet may be used only in ways that are consistent with their licenses or copyrights.

2.4.5 Any violation of this policy subjects the offender to immediate discharge and/or the reimbursement of all costs associated with such action.

2.5 File Storage

2.5.1 All electronic files should be stored either in a user's Holy Trinity OneDrive account or a SharePoint site.

2.5.2 Files should not be stored locally on a device or in another cloud platform/file server that is not operated by Holy Trinity.

2.5.3 All Personally Identifiable data must be stored in line with the guidance set out in the Holy Trinity Data Protection Policy

3 Devices

3.1 Overview

This policy is intended to protect the security and integrity of Holy Trinity's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

Holy Trinity staff must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

3.1.1 Holy Trinity grants its employees the privilege of using their own mobile device at/for work purposes at work for their convenience. Holy Trinity reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

3.1.2 Holy Trinity will provide all staff with the necessary equipment to fulfil their job role, in relation to IT this will include the use of a computer during working hours.

3.1.3 Staff should not need to provide their own computer for work purposes. In some cases, staff may choose to purchase their own laptop. If this is to be used for work purposes it is the users responsibility to ensure that the device meets all of the requirements of this policy.

3.2 Minimum Device Requirements

1.1.1 All devices used for the purposes of Holy Trinity work must conform to the standards set out in the policy.

For devices owned by Holy Trinity this will be setup by the IT administrators. For personal devices it is the responsibility of the user to ensure that before any Holy Trinity IT systems are accessed on their device it is presented to the IT administrators to ensure it meets the minimum device requirements. By giving the device to the IT administrators you agree that they will take whatever steps necessary to ensure compliance with this policy and they cannot be held responsible for the loss of any data on your device.

3.2.1 In order to prevent unauthorized access, devices must be password protected using the features of the device where available:

- The device must lock itself with a password or PIN if it is idle for five minutes.
- After five failed login attempts, the device will lock.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.

3.2.2 Employees' access to company data is limited based on user profiles defined by the System Administrator and automatically enforced.

3.2.3 The employee's device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) the System Administrator detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

3.2.4 All devices require the following security measures to be in place:

- Anti-virus software is installed and up to date
- Anti-malware software is installed and up to date
- A device firewall is active and up to date

3.2.5 Devices used for Holy Trinity must have full drive encryption to protect the data stored on it. This applies to Holy Trinity-owned devices and staff/key volunteer devices.

3.3 Device Updates

3.3.1 Holy Trinity will ensure that Holy Trinity's own devices are kept up to date with essential software updates (e.g. virus definitions, Windows updates, etc.).

3.3.2 Non-essential software will be updated at the discretion of the IT Director.

3.3.3 Users are responsible for keeping their own devices up to date and should implement manufacturer and recommended updates within a reasonable timeframe so as not to allow their own devices to become vulnerable.

Manufacturers and developers release regular updates which not only add new features, but also fix any security vulnerabilities that have been discovered. Applying these updates (a process known as patching) is one of the most important things that can be done to improve security. Operating systems, programmes, phones and apps on all devices used for Holy Trinity must be set to 'automatically update' wherever this is an option. This way devices will always be protected as soon as the update is released.

Holy Trinity recognises that all IT has a limited lifespan. When the manufacturer no longer supports a piece of hardware or software and new updates cease to appear, the device or software should be replaced.

3.4 Personal Device Support

3.4.1 Only personal devices that are used for Holy Trinity work will be supported by the IT administrators. Holy Trinity accepts no responsibility for loss of data or damage to personal devices whilst being used for Holy Trinity. Whilst the IT support team will do their best to maintain personal devices their work cannot be guaranteed.

3.4.2 Devices must be presented to an IT administrator for proper job provisioning and configuration of standard apps, such as browsers, office productivity software and security tools, before they can access the network.

3.5 Personal Device Acceptable Use

3.5.1 Holy Trinity staff agree to abide by the Acceptable Use Policy whilst their device is connected to the Holy Trinity network.

3.6 Lost or Stolen Devices

3.6.1 Lost or stolen devices must be reported to the System Administrator as soon as it is noticed to be missing, without delay. This includes all devices that have been used to access Holy Trinity IT systems whether it is owned by Holy Trinity or not.

3.6.2 When a device is reported as stolen the user will immediately change their passwords. If this is not possible their accounts will be temporarily blocked until this can happen. IT administrators will also initiate a remote wiping of the stolen/lost device.

3.6.3 Employees are responsible for notifying their mobile carrier immediately upon loss of a device.

3.7 Risks/Liabilities/Disclaimers

While Holy Trinity will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.

3.7.1 Holy Trinity reserves the right to disconnect devices or disable services without notification.

3.7.2 Staff are expected to use their devices in an ethical manner at all times and adhere to the company's acceptable use policy as outlined.

3.7.3 Staff are personally liable for all costs associated with their personal device and Holy Trinity shall not be liable for any such costs.

3.7.4 Holy Trinity reserves the right to take appropriate disciplinary action up to and including termination for non-compliance with this policy.

3.8 Portable Equipment

3.8.1 Holy Trinity owns and manages a collection of IT equipment, including projectors, laptops and tablets. All equipment is expressly for the sole use of Holy Trinity's ministry.

3.8.2 Users are expected to take precautions to ensure that laptops are not stolen, lost, or damaged.

3.8.3 If laptops are lost, stolen, or otherwise damaged such that they cannot be restored to normal working order, the employee may be responsible for the pro-rated cost of the laptop. In case of theft or loss, the user must file a report with the IT Director.

Users are encouraged to check their home insurance policies regarding coverage. Holy Trinity will evaluate the circumstances of the theft or loss to determine if the required reimbursement should be waived.

3.9 Holy Trinity owned devices

3.9.1 Laptops that are provided for church related work, must not have personal software installed on them unless approved by the IT Director.

3.9.2 Devices owned by Holy Trinity are to be used for church related work and may be used for limited personnel use.

3.9.3 Upon leaving employment or voluntary role at Holy Trinity, all equipment must be returned.

Holy Trinity keeps an asset register of all devices that they own, and each device will be assigned a unique ID. Users should know the ID of their device so that in the event of the device being lost or stolen it can be easily identified.

3.10 Reimbursement

3.10.1 Holy Trinity will not reimburse the employee for any percentage of the cost of their own device, even if it is being used for Holy Trinity work.

3.10.2 Holy Trinity may reimburse employees for reasonable costs of mobile phones subject to the discretion of the IT Director.

3.11 Plug in Devices

Plug in devices, e.g. USB flash drives, are particularly prone to carrying unseen viruses and other malicious software programmes.

As far as reasonably possible, staff and employers must not use (i.e. plug in) a device unless they are certain it has come from a trustworthy source.

3.11.1 All plug in storage devices should be scanned for malicious software before being first accessed. If anything is detected, the device should not be used and sent to the System Administrator.

3.11.2 Use of a plug in device to store data from Holy Trinity should be avoided as far as reasonably possible. However, on the rare occasion that this cannot be avoided the device must be fully encrypted to ensure security of such data in the event of the device being lost or stolen.

3.11.3 User plug in devices should be returned as soon as possible.

3.12 IT Procurement

3.12.1 The purchasing of all IT equipment must be done only after approval by the IT Director.

4 Email Communication

4.1.1 Users are provided with a Holy Trinity email for use in connection with their work at Holy Trinity, it is not to be used for personal use.

4.1.2 All use of email must be consistent with Holy Trinity's policies and procedures relating to acceptable use, ethical conduct, safety, compliance with applicable laws and proper business practices.

4.1.3 Users must not use Holy Trinity email to circulate spam messages.

4.1.4 Users must not use third-party email services (e.g. Google, Yahoo, etc.) for conducting Holy Trinity business.

Email is one of the most common methods used by hackers to initiate a cyber-attack. Users should exercise great caution when opening emails with attachments and clicking on links in emails, even if it is from a recognised source. Remember if in doubt then don't open it and seek immediate advice from the IT administrators. If a suspect attachment or link is opened, then immediately disconnect the device from the network by unplugging the cable or switching off Wi-Fi and contact the IT administrator.

4.1.5 As much as possible, personally identifiable data should not be sent via email, instead it should be submitted via electronic forms directly to the database where it is stored. Where it is necessary to do this the email must be deleted as soon as the data has been transferred to the database or file store, it must not be kept in an email folder.

Remember also that email communication is not fully secure and so it should never be used to transfer sensitive data as there is a risk of it being intercepted.

5 User Access Levels

All users will require basic access to email, membership databases and the team SharePoint site. Users may also then require access to other file servers and applications depending on their ministry area.

5.1.1 Users will be given access to data and services based on their role as determined by the IT Director.

5.1.2 All access will be reviewed on a regular basis to ensure it is in line with an individual's job role. It will also be reviewed when changing job role or department.

Access to sensitive data such as financial records or children's data should be restricted only to those who require access. For example, giving information is only available to the following people:

Full access: Treasurer, Director of Operations, Finance Manager, Deputy Operations Manager

Partial access: Office Administrator and Assistant (only relating to counting money and retail, i.e. nothing online)

Partial access: Kings Coffee House manager and assistant manager can access all financial details, less employee remuneration, relating to Kings Coffee House.

The Incumbent, as overall leader of Holy Trinity Church, may request any information at any time, though as a principle they are unaware of voluntary giving information.

5.2 Administrator Access

5.2.1 There is a requirement for those who manage the Holy Trinity IT systems to have administrator access. At all times there should be at least 2 people who have administrator access to all systems. All staff with administrator access should be deemed to be technically competent.

5.2.2 Administrative accounts should not be used for day to day work such as accessing files and emails. Staff with administrator access should have two accounts, one for day to day work and an administrator account to be used only when necessary.

This is important because an attacker with unauthorised access to an administrative account can be far more damaging than one accessing a standard user account.

5.3 Network Security

5.3.1 The Holy Trinity network will be secured by a perimeter to prevent attacks from outside the network. This firewall should be active and up to date at all times.

5.3.2 Access to the configuration of network devices is restricted to administrators and physical access to the network equipment is restricted.

5.4 Guest Wi-Fi Terms of use

5.4.1 All users connecting to the guest Wi-Fi are presented with these terms and conditions to agree to terms of use.

5.5 Connecting to a non-Holy Trinity network

5.5.1 Both personal and Holy Trinity devices that are used for Holy Trinity work are permitted to be connected to networks that are not operated by Holy Trinity when required.

When connecting to other networks users should exercise caution to not expose the device to unnecessary risk. Open networks are permitted so long as a device firewall is in place and the network is in a reputable location such as McDonalds etc. Users should however be aware connecting to any open network in a public place always carries risk so should be avoided where possible.

6 IT Disaster Recovery and Data Backup Policy

6.1 Overview

The purpose of the Information Technology Disaster Recovery and Data Backup Policy is to provide for the continuity, restoration and recovery of critical data and systems.

6.1.1 Holy Trinity will ensure that onsite critical data is backed up periodically and copies maintained at an off-site location.

The responsibility for backing up data held on the workstations of individuals regardless of whether they are owned privately or by the church falls entirely to the user.

6.1.2 All backups must conform to the following best practice procedures:

- All data, operating systems and utility files must be adequately and systematically backed up. (Ensure this includes all patches, fixes and updates).
- Records of what is backed up and to where must be maintained.
- Records of software licensing should be backed up.
- The backup media must be precisely labelled and accurate records must be maintained of back-ups done and to which back-up set they belong.
- Copies of the back-up media, together with the back-up record, should be stored safely in a remote location, at a sufficient distance away to escape any damage from a disaster at the main site.
- Regular tests of restoring data/software from the backup copies should be undertaken, to ensure that they can be relied upon for use in an emergency.

6.2 Disaster Recovery

6.2.1 Where an onsite system warrants a disaster recovery plan, Holy Trinity will put one in place within one calendar month and maintain/review it regularly.

6.2.2 Offsite data processors will have their disaster recovery plans/policies regularly reviewed.

A disaster recovery plan can be defined as the on-going process of planning developing and Implementing disaster recovery management procedures and processes to ensure the efficient and effective resumption of critical functions in the event of an unscheduled interruption.

Holy Trinity maintains contingency plans as a critical step in the process of implementing a comprehensive contingency planning program.

There are five main components of the IT contingency plan:

1. *The Supporting Information and Plan Appendices provide essential information to ensure a comprehensive plan.*
2. *The Notification/Activation, Recovery, and Reconstitution Phases address specific actions that the organization should take following a system disruption or emergency.*
3. *IT contingency plans should be clear, concise, and easy to implement in an emergency.*
4. *Where possible, checklists should be used.*
5. *Where possible, step-by-step procedures should be used.*

7 Appendix A: User Self Audit Form

Follow this check list to ensure that you are compliant with the Holy Trinity IT policy.

1. Are the passwords I am using secure and known only to me? Are they easy for me to remember but hard for somebody else to guess?
2. Is the device I am using compliant with Holy Trinity standards?
3. Does it have full drive encryption?
4. Is it password protected?
5. Does it have all of the latest software updates?
6. Does it have anti-virus, anti-malware and a firewall?
7. Am I am only using memory sticks where necessary and ensuring they are encrypted if they are being used?
8. Do I know the limitations of using email communication?
9. Am I making sure that I only store personal data in locations approved by Holy Trinity, such as ChurchSuite and the personal data SharePoint site.

8 Appendix B: Free Wi-fi Terms of Use

By accessing the wireless network, you acknowledge that you're of legal age, you have read and understood and agree to be bound by this agreement.

The wireless network service is provided by Holy Trinity Leicester and is completely at their discretion. Your access to the network may be blocked, suspended, or terminated at any time for any reason.

You agree not to use the wireless network for any purpose that is unlawful and take full responsibility of your acts.

The wireless network is provided "as is" without warranties of any kind, either expressed or implied.