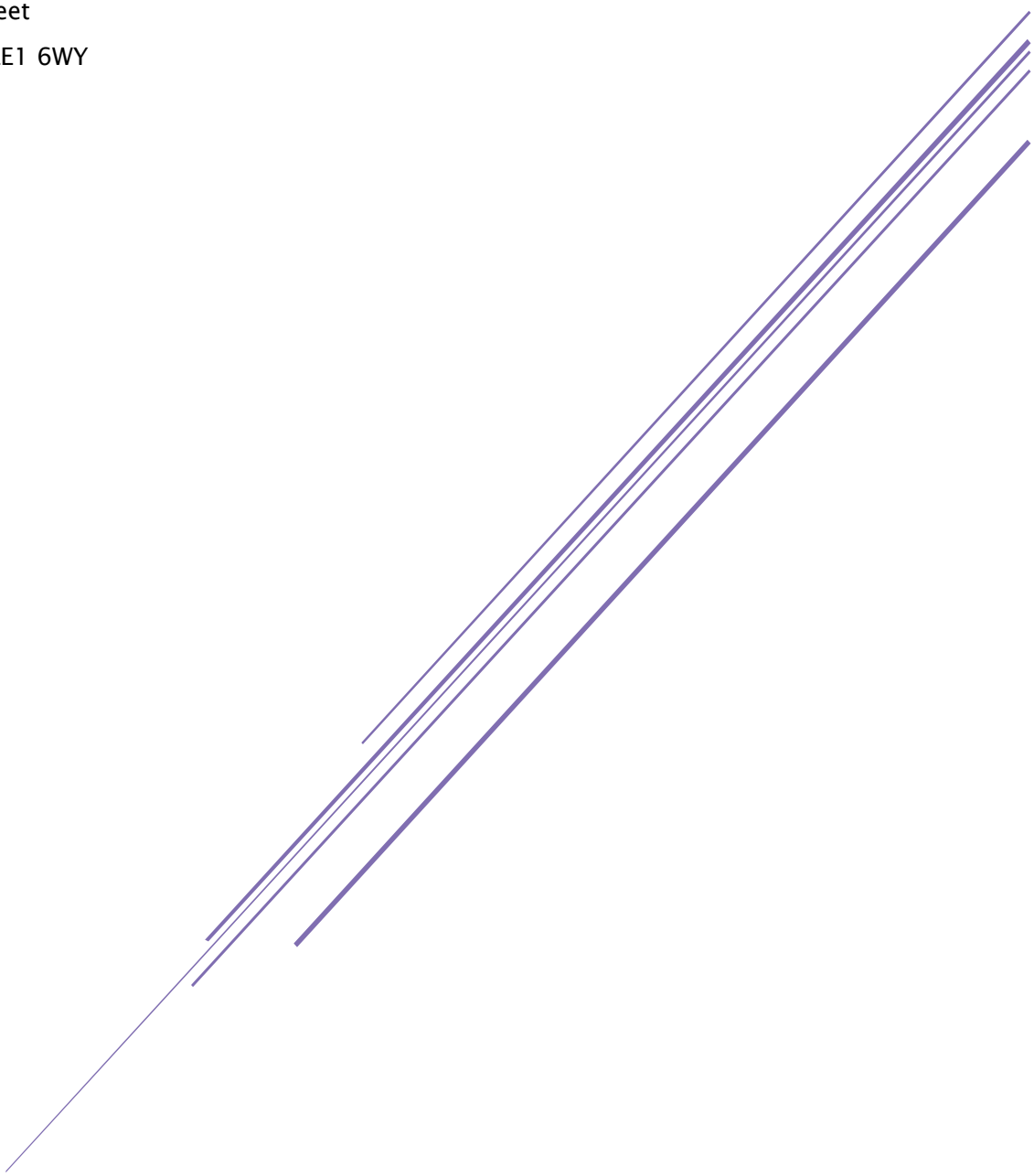
# INFORMATION TECHNOLOGY AND MEDIA POLICY

## Holy Trinity Church

Turner Street

Leicester LE1 6WY



Sep 2017

# Review History

| # | DATE | PREPARED BY | REVIEWED BY | NOTES |
|---|---|---|---|---|
| **1.0** | September 2017 | SGorton / KMaloney | | First version |
| | | | | |
| | | | | |
| | | | | |

**Review Policy**

This policy is to be reviewed at least annually by the Parochial Church Council (PCC) of Holy Trinity Church, or when significant changes in Law requires it. Furthermore, should any significant incident occur where IT usage has contributed to the problem, it is advised strongly that the policy be reviewed at that point.

# 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).

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. 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 may result in disciplinary action.

# 2 Data Protection

Holy Trinity is committed to uphold, respect, and protect the privacy and confidential information of Members, Friends and the Church. The Church will not share membership lists and member information with outside parties. Holy Trinity will not divulge personnel information to outside parties except as required by Law, or appropriate judicial order.

Everyone is expected to play their part in keeping our information secure and abiding by this Policy. Understanding your responsibilities will ensure you remain safe when using the internet, email or your workstation.

## 2.1 Introduction

**Stephen Gorton** is the Data Controller for the purposes of the Data Protection Act on behalf of Holy Trinity.

Holy Trinity uses personal data about living individuals for the purposes of general church administration and communication.

Holy Trinity recognises the importance of the correct and lawful treatment of personal data. All personal data, whether it is held on paper, on computer or other media, will be subject to the appropriate legal safeguards as specified in the Data Protection Act 1998.

Holy Trinity fully endorses and adheres to the eight principles of the Data Protection Act. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. Employees and any others who obtain, handle, process, transport and store personal data for Holy Trinity must adhere to these principles.

## 2.2 The Principles

The principles require that personal identifiable information (PII) shall:

1. Be processed fairly and lawfully and shall not be processed unless certain conditions are met
2. Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose
3. Be adequate, relevant and not excessive for those purposes
4. Be accurate and, where necessary, kept up to date
5. Not be kept for longer than is necessary for that purpose
6. Be processed in accordance with the data subject's rights
7. Be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measures, and:
8. Not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Any storage of PII on portable devices (e.g. laptops, tablets, phones, USB sticks, etc.) must be authorized by the Data Controller and consideration will be given to the security afforded to such data. Any break of this may result in disciplinary action.

## 2.3 Maintaining Confidentiality

Holy Trinity will treat all your personal information as private and confidential and not disclose any data about you to anyone other than the clergy, employed staff, authorised leadership and ministry overseers/co-ordinators of the church in order to facilitate the administration and day-to-day ministry of the church.

Information and data stored by the Church Office will not be distributed in any form such as digital, hard copy or any other form, which might breach the Data Protection Act.

Your personal information will not be given or sold to any other person, company or church.

All employed staff are required to sign a confidentiality clause written into their contract of employment.

All clergy, employed staff and authorised leadership and ministry overseers/co-ordinators who have access to personal data obtained under this policy will be required to agree to and sign this Data Protection Policy.

There are four exceptional circumstances to the above permitted by law:

1. Where we are legally compelled to do so
2. Where there is a duty to the public to disclose
3. Where disclosure is required to protect our interest
4. Where disclosure is made at your request or with your consent

## 2.4 Use of Personal Information

Holy Trinity will use personal data for four main purposes:

1. The day-to-day administration of the Church including pastoral care and oversight, calls, emails and visits, preparation of ministry rotas, maintaining financial / giving records for audit and tax purposes
2. Contacting you to keep you informed of church news, activities and events
3. Statistical analysis to gain a better understanding of church demographics
4. With your specific permission, for the production of a church contact list which will be made available to other members of Holy Trinity.

Data will be held whilst you are a member of the church and destroyed 18 months after you leave the church or we receive a written request from you. The exception to this will be where need to keep statutory records for a longer period.

## 2.5 Membership Databases

Membership Information is held on the Church Membership Database. This is currently held in the ChurchSuite cloud-based software system and is accessible by computer and mobile device only. Data held is kept safe and secure (details of the security can be found at https://churchsuite.com/tour/security).

Access is by registered users only along with individual passwords. All authorized users should follow the password policy (see section 5.1 Passwords).

Access by registered users is logged by ChurchSuite and the list of authorized users is reviewed every 6 months. Authorization levels are maintained to ensure that each user can see only what they need to see.

.

### 2.5.1 Charitable Giving Data

Further information specific to financial giving (e.g. names, addresses and Gift Aid declarations) are stored in a local Sage Accounts software programme. This is accessible only by the Data Controller, Treasurer and Finance Assistant for the purposes of accounting and financial management only. Access is via a 3-step password process.

Some financial information is kept on ChurchSuite, by means of uploading reports generated by our online banking system. Instructions for this are as follows:

- Such downloaded reports must be kept securely and deleted when finished with.
- These reports may not be shared with anyone other than the Data Controller, Treasurer and Finance Assistant.
- The downloaded reports must be cleaned of all non-essential data, including all outgoing payments, ticket sales information and bank balance.
- No remaining data should be modified in order to maintain accuracy, although structure may be modified to best suit the uploading process.
- The report may only be uploaded to ChurchSuite and no other system.

### 2.5.2 Member Data

Members of Holy Trinity Church who are listed in the database may access their personal information, and that of their registered children, from the "My ChurchSuite" system, a client-facing part of ChurchSuite. Members should be unable to view data of other users without their express permission.

Information collected by the Church Office will be stored on the Database and will not be used for any other purposes than set out in this section.

1. Access to the Database is strictly controlled through the use of name specific passwords, which are setup and authorised by the Data Controller.
2. Only the clergy and church staff and authorised leadership and ministry overseers/co-ordinators have access to the full database.
3. The Database will NOT be accessed by any authorised users outside of the EU, in accordance with the Data Protection Act, unless prior consent has been obtained from the individual whose data is to be viewed.
4. Personal information will not be passed onto any third parties outside of the church environment.
5. Personal information may be made available to others within the church environment via the password protected members area of the church website with the express permission of the data subject who will be given the opportunity to 'opt in' to this. This information may also be published in a church contact list which will be made available, via the office, verbally or in paper form to church members without website access.
6. The need to process data for normal purposes has been communicated to all data subjects. In some cases, if the data is sensitive, for example information about health, race or gender, express consent to process the data must be obtained.

## 2.6 Storage of Data on Other Media

All clergy, employed staff and authorised leadership and ministry overseers/co-ordinators who store personal information obtained under this policy on any electronic system not connected to the Holy Trinity computer network or part of the Holy Trinity website are required to do so

in accordance with the principles of the Data Protection Act and to take due care to ensure that the information remains secure through the use of passwords and encryption where appropriate. This includes:

- Email / telephone / address books held on personal computers, mobile phones, tablets, etc.
- Data stored on memory sticks and/or portable hard drives

## 2.7 Rights to Access Information

Employees and other subjects of personal data held by Holy Trinity have the right (with some legal exceptions) to access any personal data that is being kept about them either electronically or in paper-based filing systems. This right may be withheld if the personal information also relates to another individual.

Specifically, all individuals who are the subject of personal data held by Holy Trinity are entitled to:

- Ask what information the church holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed what the Church is doing to comply with its obligations under the 1998 Data Protection Act.

Any person who wishes to exercise this right should make the request in writing to the Data Controller, using the standard letter which is available on-line from www.ico.gov.uk. Holy Trinity reserves the right to charge the maximum fee payable for each subject access request.

Holy Trinity aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of a completed form unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

If personal details are found to be inaccurate, they can be amended upon request.

## 2.8 Photographs and Videos

For the purpose of simplicity, the word “Photography” refers to the collection of static or moving images. This section is considered due to the ease of which such data can be collected digitally and shared quickly.

Photography of under 18s is covered in the policy “Holy Trinity Child Protection Policy Revised May 2017”.

Photography of vulnerable adults is covered in the policy “6 Safeguarding Adults Policy updated for PCC July 2017”.

Where photography does not involve under 18s or vulnerable adults, the following will apply.

Only authorized photography is allowed. Staff, trustees or those in leadership are given authority to ask any person taking photos to stop and delete them if they believe this to be appropriate. Should that person unreasonably refuse, they are to be requested to leave the premises and the Police may be contacted should that be appropriate in the situation.

Photographs taken within the Church building or at Church events may include individuals or groups of individuals attending these events. These photographs will be used solely for the

purpose of Holy Trinity advertising, marketing and public relations, and may thus appear in any advertising internal and or external, website or other publicity material.

The Data Protection Act DOES apply where photographs are taken for official use, such as for identity passes, and these images are stored with personal details such as names. Where the Act does apply, it will usually be enough for the photographer to ask for permission to ensure compliance with the Act, prior to photographs being taken.

Photographs taken at Holy Trinity purely for personal use are exempt from the Data Protection Act. This means that parents, friends and family members can take photographs for the family album of their children and friends participating in church events.

## 2.9 Website Privacy Statement

The following statement is provided for users of the www.holytrinityleicester.org website:

At Holy Trinity we collect different types of information about our users for the following main reasons:

1. To provide an interactive web site where email is used to communicate with the users.
2. To provide a security mechanism whereby we can restrict content to certain groups of users.
3. To help us to improve the service we offer.

**Our Principles**

We are absolutely committed to protecting your privacy. Our policy can be summarised in one sentence: we will not share your information with others without your consent.

We have established the following three principles:

1. We will respect your email privacy. You will only receive email from Holy Trinity in relation to areas you have expressly signed up for.
2. All group emails will be sent as bcc… to protect your privacy.
3. We will not share any individual user details (including your email address) to any third party without your consent.

**What information do we collect?**

- We collect information on our users through registration.
- The minimum information we need to register a user is your first and last name, your postcode and a password.

**Who will have access to your information?**

- You have control over who is able to access specific items of information.
- By default, your information will not be visible to anyone else using the site.
- You can change these settings from your personal profile page.

**What else you should know about privacy**

- Remember to close your browser when you have finished your user session. This is to ensure that others cannot access your personal information and correspondence if you share a computer with someone else or are using a computer in a public place like a library or Internet cafe. You as an individual are responsible for the security of and access to, your own computer.

- Please be aware that whenever you voluntarily disclose personal information over the Internet that this information can be collected and used by others. In short, if you post personal information in publicly accessible online forums, you may receive unsolicited messages from other parties in return. Ultimately, you are solely responsible for maintaining the secrecy of your usernames and passwords and any account information. Please be careful and responsible whenever you are using the Internet.
- Our pages may contain links to other websites, and you should be aware that we are not responsible for the privacy practices on other websites.

# 3 IT Disaster Recovery and Data Backup Policy

## 3.1 Objective

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.

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

Holy Trinity will maintain a written continuity plan for critical assets that provides information on recurring backup procedures, and also recovery procedures from both natural and man-made disasters.

## 3.2 Scope

Staff users are responsible for arranging adequate data backup procedures for the data held on their own devices. The Data Controller can provide advice to staff users on request.

The System Administrator is responsible for the backup of data held in central systems and related databases. The responsibility for backing up data that resides on other systems, regardless of whether they are owned privately or by Holy Trinity falls entirely to the user.

## 3.3 Data Backup

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.

## 3.4 Disaster Recovery

A disaster recovery plan is 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.

# 4 Device Policy

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.

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.

## 4.1 Personal Devices and Support

Smartphones including iPhone, Android, Blackberry and Windows phones are allowed.

Tablets including iPad and Android are allowed.

A regular audit of such devices shall be carried out by the System Administrator at least once per year.

Connectivity issues are supported by the System Administrator; employees should/should not contact the device manufacturer or their carrier for operating system or hardware-related issues.

Devices must be presented to System 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.

## 4.2 Personal Device Acceptable Use

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

## 4.3 Portable Equipment

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

Users are expected to take precautions to ensure that laptops are not stolen, lost, or damaged. 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 (first year: 100%; second year, 75%; third year, 50%; fourth year, 25%). In case of theft or loss, the user notify the Data Controller immediately.

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.

Because laptops are provided for church related work, no personal software may be installed unless approved by the Data Controller. Laptops are purchased to be used for church related work and may be used for limited personnel use.

## 4.4 Reimbursement

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.

Holy Trinity will pay a monthly amount to each staff member, above salary, to cover appropriate mobile phone usage. Holy Trinity will not reimburse staff for the following charges: roaming, plan overages, etc.

## 4.5 Security

In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password (see section 5.1 Passwords) is required to access the company network.

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 being used by the employee for church purposes.

Smartphones and tablets that are not on the company's list of supported devices are not allowed to connect to the network.

Smartphones and tablets belonging to employees that are for personal use only are allowed to connect to the network.

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

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. This functionality must be enabled by the user.

It is the responsibility of the employee to ensure their personal device has security provisions, e.g. anti-virus, anti-malware and firewall applications, prior to connecting to the Holy Trinity network. The minimum provision is anti-virus software that is kept up to date. Such software is widely available including:

- Sophos (Windows, Linux and Android anti-virus)
- AVG (Windows anti-virus)
- Norton Internet Security (Windows-based security)
- McAfee Security
- Malwarebytes (Windows-based anti-malware)
- Windows Defender (anti-virus for Windows 10)
- Microsoft Security Essentials (anti-virus for Windows 7)

Where adequate software is not available freely to comply with our requirements, Holy Trinity will cover the cost of what is necessary and appropriate.

### 4.5.1 Encryption

Devices used for Holy Trinity work should have full drive encryption to protect data in the event of the device being lost or stolen. This applies to Holy Trinity-owned devices and staff/key volunteer devices.

The minimum encryption level should be 256 bit key, 128 bit block.

Encryption passwords or pass phrases should comply with the password policy (see section 5.1 Passwords).

Software such as BitDefender is recommended but will be considered on a case-by-case basis by the Data Controller.

## 4.6 Risks/Liabilities/Disclaimers

While Holy Trinity will take precautions 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. where such items are related to Holy Trinity work. Any stored backups by the employee must follow the data storage policy (see section 2.6 Storage of Data on Other Media).

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

Lost or stolen devices must be reported to the System Administrator within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.

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

Staff are personally liable for all costs associated with his or her device.

Staff assume full liability for risks including, but not limited to, the partial or complete loss of Holy Trinity and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

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

## 4.7 Holy Trinity Wi-Fi

Holy Trinity's Wi-Fi connections are available to staff for personal use within the terms of these guidelines and any terms and conditions you accept when you connect to the service.

## 4.8 Live TV

If you want to watch live TV, or programmes on BBC iPlayer, on your personal mobile device (providing it is not connected to the mains) on Holy Trinity premises you must make sure you are covered by your own TV Licence.

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.

## 4.9 Courtesy Guidelines

The following guidelines are mainly for staff members in regards to use of personal devices for personal reasons during working hours.

### 4.9.1 Ringtones

Quiet ringtones are welcome in the office. Mobile telephones should not provide a point of distraction for other staff.

### 4.9.2 Taking Calls

Personal telephone calls should be kept to a minimum, but when they are appropriate then care should be taken to ensure that other staff are not disturbed.

### 4.9.3 General Noise

Do not play content with loud audio that will be heard by those around you.

### 4.9.4 Safety

Caution should be exercised when using devices, particularly if on the move, and be respectful to colleagues.

It is illegal to use a hand held device when driving, and staff are not obliged to make or receive work calls if their vehicle has been fitted with hands free kit.

### 4.9.5 Meetings

During meetings, phones should be set to silent and preferably only answered if absolutely necessary.

### 4.9.6 Manners

Ongoing conversations with colleagues should not be interrupted by phone calls unless it is very urgent.

### 4.9.7 Confidentiality

It is not appropriate to use your personal mobile device to record conversations with others unless agreed with them in advance.

### 4.9.8 Images

Appropriate imagery should be used as backgrounds, screensavers, etc., as this is visible by staff, visitors and members of Holy Trinity.

## 4.10 Plug in Devices from Untrusted Sources

Plug in devices, e.g. USB flash drives, are particularly prone to carrying unseen viruses and other malicious software programmes. Our policy for the use of such devices is as follows:

- As far as reasonably possible, do not use (i.e. plug in) a device unless you are certain it has come from a trustworthy source.
- 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.
- Use of such devices must follow the general Device Use Policy (see 4.2 Personal Device Acceptable Use).

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

# 5 Computer Use Policy

## 5.1 Passwords

Passwords should be strong: comprising a combination of upper case letters, lower case letters, numbers and special symbols, with a minimum count of 8 characters (no spaces) and preferably 16 characters.

Passwords will be changed every 6 months (preferably 3 months).

Passwords will not be shared; this includes the staff Wi-Fi network keys.

Such requirements will be enforced where possible on the system infrastructure (e.g. Exchange Online and Windows Server Active Directory).

## 5.2 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.

The underlying philosophy of this policy is that Internet access from Holy Trinity is primarily for church-related purposes including communicating with church members and colleagues, researching relevant topics and obtaining useful business information. In addition, all existing laws and Holy Trinity policies apply to an employee'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.

Computer users are reminded that the Internet is not a secure method of communication. Neither proprietary information nor any information received in confidence by Holy Trinity, or the user, may be sent on the Internet unless prior approval is received from the Vicar or the Operations Manager.

Internet usage is monitored and suspicious usage may be investigated, potentially leading to disciplinary action.

### 5.2.1 Suspicious Emails

Should staff receive suspicious emails, they are required to do the following:

- Do not click on any link contained within the email.
- Show the email to the Data Controller (not forward it to them) and seek their guidance.

In most cases it will suffice to delete the email fully (not just transfer it to the Bin or Junk folder).

Should a link be inadvertently activated, this should be reported immediately to the Data Controller.

### 5.2.2 Explicit Prohibitions

Users are reminded that their use of the Internet will be directly traceable to our Internet address. We therefore ask staff and users not 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

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 Operations Manager.
- 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.

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

Holy Trinity will take reasonable steps to block any site that it deems inappropriate. However, we 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.

## 5.3 Privacy

Users should not have any expectation of privacy as to his or her Internet usage. It is possible to monitor Internet usage patterns and Holy Trinity will regularly inspect any and all files stored on Holy Trinity resources to the extent necessary to ensure compliance with the Acceptable Use Policy.

Where non-compliance has been found, this could be investigated and lead to disciplinary action.

## 5.4 Software

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.

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.

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 Operations Manager, and must arrange to have such software properly licensed and registered.

Users may 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.

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

# 6 Social Media

Holy Trinity generally views creating or contributing to personal websites, blogs, social networks, message boards, virtual worlds, and other kinds of social media positively. We recognize the desire of many of our staff and appointed volunteers to participate in online community and encourage this form of networking and idea exchange.

As a member of Holy Trinity staff, you may be seen by our members, attendees, and outside parties as a representative of our organization. This means that while you may view your online presence as a personal project, many readers will associate you and the views you express with us. In light of that, we ask that you observe the guidelines outlined below.

Please keep in mind that these guidelines will continue to evolve as new social networking technologies emerge. Check back periodically to ensure that you are up-to-date. If you have questions, please contact the Operations Manager.

## 6.1 Protecting Your Information

Criminals and fraudsters can use social media to find out personal information that they can use to try to compromise security checks, or to make inappropriate contact with you or other colleagues. This is called social engineering.

To minimise the risk of this happening where you are using social media for professional reasons – for example LinkedIn - we recommend that you only include high level professional information in any online profile. For example, that you work at Santander UK but not the details of your specific job role or where you are based at work.

Please approach social media sites in the same way you would when communicating and networking in the physical world - using your judgement and common sense.

## 6.2 Personal Website

If you have a personal website or blog or are considering creating one, please discuss this with your supervisor or team leader. If you have any questions, feel free to contact the Operations Manager.

### 6.2.1 Include a Disclaimer

Include this or a similar statement on your blog home page or in a prominent location on your social media site:

*The posts on this site are my own personal opinions. They are not read or approved by Holy Trinity before posting and do not necessarily represent the views and opinions of Holy Trinity.*

## 6.3 Maintain Confidentiality

Ask permission before reporting on conversations or meetings that are meant to be private or for internal use only. Do not disclose any information, pictures, or videos that are confidential or proprietary to Holy Trinity. This includes information that will become public, but has not yet been announced or posted.

## 6.4 Copyright

All Holy Trinity environment names, copyrights, and trademarks are the property of Holy Trinity and should be used according to our guidelines.

You may embed or link Holy Trinity-owned video, graphics, or other materials, including program or line-cut video from services or events, to your site if they have been posted publically by Holy Trinity on ministry-owned websites or blogs.

In all cases, Holy Trinity should be credited for the materials and the credit should include © *<year created> Holy Trinity Church*, and the speaker/author. Otherwise, Holy Trinity-owned material should not be posted on your site.

You may use up to 250 words of Holy Trinity print media (unedited and within your own commentary or with other quotes on a page) from any published Holy Trinity work. Holy Trinity should be credited for the material and the credit should include © *<year created> Holy Trinity Church*, and the author. Please do not post any content that is the property of another individual or company unless you have written permission or are sure that the use of the material is legally permitted.

This is your responsibility; we cannot provide you with legal advice regarding copyrights.

## 6.5 Good Judgment

Remember that what you write is public. You should always assume that it will be read by your boss, your co-workers, church volunteers and attendees, other church leaders, your parents, your children, your spouse, and the solicitor for the person who doesn't like you. Ask yourself if you are comfortable with all of these people reading what you plan to post. What you write is your responsibility and you are legally responsible for your comments.

Write as yourself. Use your real name. If you choose to identify yourself as an employee of Holy Trinity or to discuss anything related to the organization, be clear about your role. Be accurate in what you write and ensure that you have all the facts about your subject. If you make a mistake, admit it and be quick to correct it. Be careful that what you write would not impair your ability to work with your staff team, lead your volunteer teams, speak with credibility to other churches, or represent us in the community.

Remember that frustrations are best expressed in person. Sarcasm does not usually translate well, so be careful how you use humour. Respect your audience. Be thoughtful. Don't refer to volunteers, attendees, or vendors' name without permission. Don't post pictures of others without permission. Don't use ethnic slurs, personal insults, obscenity, or engage in any conversation that would not be acceptable in our workplace.

Choose your topics wisely. There are some ideas that are best discussed in a personal conversation rather than a public forum. These might include political views and the church's stance or policy on certain topics. Don't allow your posts to hinder someone's spiritual growth.

Remember that what you write, even if retracted, is archived and can be with you longer than you might expect.

## 6.6 Refer Press Enquiries

Your posts may generate media coverage. If a member of the media contacts you about a Holy Trinity-related post or requests Holy Trinity information of any kind, contact your Ministry Team Leader or supervisor for direction on how to respond.

## 6.7 Advertise Wisely

Should you choose to advertise on your site, to the extent you have control, ensure that the adverts are consistent with our values.

## 6.8 Make use of the Employee Handbook

The Employee Handbook offers more detail about our Standards of Conduct. Contact the Vicar or Operations Manager if you have any questions.