IT Policy & Procedures

This document describes the IT equipment and facilities used by St Luke's Church and the procedures, rules and guidance necessary to keep them working and to keep both hardware and data secure.

"Computer" refers to any device that can access data – PC, Mac, tablet or smartphone.

"Data" refers primarily to church data that is classed as personal, confidential or sensitive.

The Trustees are responsible for St Luke's IT and data. They delegate that responsibility to the IT group, part of the Compliance Subgroup. The Compliance group should be consulted for authorisation to access and handle data, including on personal devices. The Trustees may view activity on church systems and allow or deny access.

A guidance document on security, including passwords, email etiquette and recognising scams, will be available separately on the church website and from the office. It is useful for anyone using IT for personal, church, or business purposes and should be read alongside this policy.

1. Data security

1.1. Data security and the law

The church holds data that is legally classed as *personal data* (eg names and contact details) and as *sensitive personal data*, which includes a person's religion (ie church membership) and is covered by further rules. The precautions outlined here, and in the Privacy statement and other guidance, are essential for the church to comply with the law.

The law includes data on paper (eg contact lists), which must also be managed with due care, not left in public or otherwise accessible to unauthorised persons. It must be destroyed when no longer in use.

Anyone handling personal data in any form must be fully aware of relevant church policies:

Data Privacy Statement (GDPR)

Retention of Records

Digital Communications with Under 18's Policy

1.2. Breaches of Security

On becoming aware of, or suspecting, a breach of security of any kind, or realising that a security breach is in progress or that there is a future risk, a member of the Compliance Subgroup, Churchwarden or Minister must be informed immediately.

A security breach means anything likely to compromise the church's computer systems and data e.g.

- loss of a PC or laptop containing church data (whether the church's or your own),
- mistakenly revealing a password,
- losing or mis-filing data in a way that may make it available to others,
- sending a sensitive email to the wrong recipient,
- noticing a malfunction on a PC or laptop that could affect access to data,
- unexplained loss or corruption of data,
- defacement of the Web site,
- finding an unknown person in the office,
- having responded to a malicious 'phishing' email* (see guidance note),
- anything else that arouses suspicions around the security of personal data.

**Simply receiving and deleting a suspicious email is not a data breach, but others should be warned to watch for it.*

1.3. Data extracted from secure cloud storage

Most of the personal data held by the church is the secure cloud-based service, Churchsuite.

It is sometimes necessary to save data from Churchsuite (reports, lists, printed items) on local computers or on paper. Such datasets must only be handled outside of Churchsuite if the task is essential, and the user

is authorised to do so. Church staff and officers using church computers are authorised. Church personal data may not be saved on personally-owned devices without a clear need and specific authorisation.

Such data must be kept secure, including password protection and physical security of the device used. The user must understand where the files are saved and be able to fully delete all copies of the material, which they must do as soon as the task is complete.

Church data may not be stored on Cloud services, other than Churchsuite or the church Sharepoint facility.

1.4. People are the greatest risk to IT security.

Despite all technical measures, personal vigilance is vital to prevent unauthorised access to data or its destruction. Emails and other forms of deception to obtain passwords and data are a constant threat. 'Phishing' emails are the most common risk, designed to entice the recipient to make a response or click a link that leads to the disclosure of a password.

All IT users – church or personal - should be aware of the issues explained in the guidance document.

2. Description of equipment and facilities

2.1. Hardware

Church computers are connected to a network, giving access to a printer and via broadband to the internet. The church does not have a central 'system' or server. Cloud services accessed via the internet provide shared storage.

The church has the following IT equipment:

- PCs in the main offices,
- Laptops used mainly by specific staff and volunteers.
- PCs in the worship area, for audio-visual use, along with other AV equipment.
- Portable data projectors.
- A shared printer/scanner/copier

Access to each computer is managed via personal passwords.

Users of the building may be given the WiFi password to enable access to the internet. This does not give access to any church computers or data.

2.2. Online data storage and services

- Shared storage is in Microsoft 365 Sharepoint. This contains all general and confidential filing. Access to confidential items is restricted to a very few specific users with relevant roles.
- Church email accounts are provided via Microsoft 365 and have addresses in the domain *@slclm.org*.
- A database of personal contact data on church members, room booking etc. is managed via Churchsuite. This is an online software service using its own secure cloud and its own personal login/password security.
- Financial data is managed via a secure cloud-based service from Data Developments.
- The church website is hosted by a separate commercial service and contains only public information.

3. Using church IT facilities

Authorised users have access to the above services via personal login names and passwords.

- The office PCs are mainly used by the Administrators. One is also used for heating management.
- The Youth and Children's leader and children's volunteer each have a church laptop.
- The Minister, Wardens, Trustees and other church officers and volunteers use their personal computers or mobile devices for church business, under the terms in this document.
- Many of the above have access to the 365 Sharepoint storage and use a church email address.
- A few staff and post-holders have access to Churchsuite, the online membership and booking database.
- The small Finance team have access to the cloud-based financial data.
- The AV team use the DP and streaming computers, often via remote-access software. These computers do not hold church data.
- In due course, all members of the congregation may be offered basic access via their browser to view and edit their own personal data (only) on Churchsuite.
- All access to online services and computers holding personal or confidential data is via individual usernames and passwords and restricted to authorised persons.

All users of church equipment and online facilities must set strong personal passwords and keep them secure - see the accompanying guidance document.

3.1. Rules and procedures for users of church equipment

All users of church computers are expected to:

- Understand the issues around security, passwords and email – outlined in the guidance document.
- Set a 'strong' personal password (ideally three random words) and not share it with others*.
- Treat all church equipment with due care.
- Use church equipment only for church business, with limited personal activity as noted below.
- Not install software or hardware or interfere with installed anti-malware unless authorised to do so.
- Not connect storage devices (memory sticks etc.) unless their origin and content is known and trusted.
- Log out when leaving a computer unattended for an extended time.
- Respect the licensing terms of any software.
- Turn off monitors at the end of a session (some PCs are required to be left on, but logged out).
- Report any concern, technical fault or other issue to the IT group or a warden. *If personal data is at risk (ie an unauthorised person could gain access to it) this is an urgent and serious matter.*

*Shared usernames may be used on the AV computers, as there is no access to church data.

3.2. Portable devices provided by the church

These may contain small amounts of personal or confidential information and must be managed accordingly.

- They must not be lent to or used by any unauthorised person, including family or friends.
- They must not be left unattended in a public place or left visible in a (locked) parked car.
- They must not be used on a public WiFi connection except via a secure connection (VPN).
- The password protection and anti-virus software must always be active.
- They remain the property of the church and must be returned, or occasionally shared with other authorised users, when required.

3.3. Personal use of church equipment

Occasional personal use of church IT equipment is permitted, provided that:

- Such use does not take priority over work responsibilities or hinder the work of others.
- Church data is not used for personal purposes.
- The personal nature of any external communication is made clear.
- There is no potential for expense, negative impact or reputational damage to the church.
- There is no downloading of software, or engagement in inappropriate online activity.
- The church reserves the right to withdraw this benefit at any time.

3.4. Software licensing

Proprietary software licensed by the church is for church purposes only. It may not be installed on personal equipment unless clearly authorised and used for church purposes. Misuse of licensed software is illegal.

3.5. Remote access

This refers to the use of remote connection tools to access an on-site church computer from off-premises. It is normally used for AV setup, heating control or fault-finding purposes.

- Such connection must only be made by authorised persons.
- Personal or sensitive data must not be transerrred.
- The church accepts no liability for any risk to the user's remote device.

3.6. Church WiFi and internet

The church WiFi network serves the whole building. Trusted users of the building may be given the WiFi password. It does not provide access to any church computer or data.

The church internet connection must not be used for any activity that is illegal, offensive or likely to have negative repercussions for the church or its reputation.

Users must not upload, download, use, retain, distribute or disseminate any images, text, materials or software which might be considered indecent, offensive, unlawful, defamatory or otherwise incur liability or reputational damage to the church.

4. email

Church email accounts (in the domain *@slclm.org*) are provided to enable internal and external communication on church business. Wherever possible, church email addresses should be used instead of personal ones for official – especially external - church business. However, many volunteers use their personal email to communicate on internal church business. They should also follow the rules below.

The guidance document on passwords, scams and email etiquette should be read carefully by all email users.

Some volunteers share a personal email address with their spouse and must take note of any confidentiality issues.

4.1. Use of church email

Church email facilities must not be abused in any way, including:

- Sending unsolicited emails (spamming) or unsuitable, defamatory or illegal material.
- Use for purposes unrelated to one's role/activity.
- Spoofing (pretending to use) other people's email accounts.
- Opening or reading email which has an unacceptable risk e.g. embedded virus.
- Receiving email without using a suitable email-aware anti-virus system.
- Rules for the use of the church internet connection are also relevant for email.

4.2. Email content

- Take care what you say in an email. All expressions of fact, intention and opinion via email have the same status in law as if they were spoken or in writing. They could therefore be used legally against the sender or the church. Do not include anything in an email which you cannot or are not prepared to account for.
- Email messages which have been deleted from the system can be traced and retrieved so any offending email can be identified.

The following text must be appended as signature on all emails to external addresses on church business:

The contents of this email and any files transmitted are confidential and are solely for the intended addressee(s).
If you have received this email in error, kindly notify us immediately and delete the message from your system.
Any views or opinions expressed within this email are solely those of the sender and do not represent those of the trustees of St Luke's Church, unless otherwise stated, nor should it be taken to create any legal relations, contractual or otherwise.
The sender does not accept liability for any errors or omissions in the content of this message nor for any damage sustained from viruses which may arise as a result of the email transmission.
St Luke's is a Local Ecumenical Partnership between Anglican, Baptist, Methodist and United Reformed Churches in Lodge Moor. Registered Charity No 1136795

4.3. Confidential communication via email

- Ensure that the recipient is comfortable with this means of communication – remember that other persons may have access to the recipient's messages. If the content is highly confidential, phone or speak to them to agree on the best way to communicate securely.
- Treat electronic information with the same care as you would confidential paper-based information. Keep emails secure, use the content only for the purpose(s) intended and do not disclose content to any unauthorised third party, which may include colleagues.
- When deleting confidential emails from the inbox, also delete them from any other folders where your mailer may have placed them. Possible examples are Junk, Trash, Spam, Archive, Bin, Deleted.
- Only print confidential emails and attachments if essential and do not leave confidential print where others can read it – including on the printer. Do not retain confidential print-out when no longer needed - store or destroy it appropriately.