Stopsley Baptist Church

IT & Acceptable Usage Policy

Date: 04/08/2021

Owner: Stopsley Baptist Church

Table of Contents

1 Definitions & References

1.1 Definitions

"Stopsley Baptist Church"	SBC
"GreenHouse"	GH
"Information System"	This is Stopsley Baptist Church's hardware (servers, workstations, printers, scanners, etc.), software, network infrastructure and the data stored/associated with them including external services which Users are required to use as part of their role.
"User"	This refers to all staff, permanent or temporary, on contract or employed by third parties, and volunteers who use the building and or services provided by the church.
"IT Administration"	This refers to IT Administration who are responsible for Stopsley Baptist Church Information Systems.
"MUST/SHALL"	The statement is an absolute requirement.
"MUST NOT/SHALL NOT"	The statement is an absolute prohibition.
"MAY"	The statement is a truly optional requirement.
"SHOULD"	Use of this term indicates that there may be valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
"GHM"	GreenHouse Mentoring

2 Introduction

This policy applies to all Users and to all Information Systems owned or leased by SBC.

The purpose of this policy is to outline the acceptable use of computer and telecommunications equipment at Stopsley Baptist Church, Luton. These rules are in place to protect the Users and Stopsley Baptist Church. Inappropriate use exposes Stopsley Baptist Church to risks including virus attacks, loss of confidential data, compromise of network systems and services, and legal issues.

Information security is no longer a technical issue but a business enabler. The challenge is to adapt it to the business objectives by developing a comprehensive information security strategy encompassing governance, risk management and compliance. It is a top-down process that begins with support and commitment from the management. Stopsley Baptist Church's Management has agreed to adopt a culture of information security in its business/charity activities.

Information security is everybody's responsibility. It goes without saying that security is not complete without support from all parties. We seek the involvement, participation and support from all Users.

All Users must acknowledge and sign this acceptable usage policy before gaining access to SBC's Information Systems.

2.1 Policy Authority

Written By	Version/ Date	Comments
Christopher Young	4 Aug 2021	Policy Created

3 Policy

3.1 General Use and Ownership

3.1.1 Information Systems are provided to assist Users in carrying out their duties. Although reasonable personal use is permitted, Users shall ensure this personal use does not impede or affect their work and that their usage is in line with this policy.

3.1.2 All information created on Information Systems shall remain the property of SBC.

3.1.3 Confidentiality of User's personal information on Information Systems is not guaranteed. Users should avoid storing personal information on company machines.

3.1.4 For security, administration, and compliance purposes, authorized individuals (IT Administration or Executive Director) within SBC may monitor Information Systems, system usage logs and the data stored on those systems at any time.

3.2 Information Classification and Protection

3.2.1 Users should take all necessary steps to classify the information and ensure suitable controls are in place to prevent unauthorized access to that information. This policy requires information to be classified as follows:

- Public information. Information available on the web or provided for public consumption. Classification label: "Unclassified", "Public" or no label.
- SBC internal information: material whose disclosure would cause light to moderate damage to the affected party. e.g. internal memos, minutes, etc. that are not for public consumption. Classification label: "Internal".
- SBC restricted information; access for defined Users, roles or User groups, according to specific rules; material whose disclosure would cause serious damage to the affected party, e.g. HR data, sensitive constituent data, etc. Classification label: "Restricted"
- SBC confidential information; limited access to a very small set of persons; material whose disclosure would cause severe damage to the affected party, e.g. Safeguarding disclosures, sensitive personal discussions, Trustee/executive/minister level management changes, financial details, strategic decisions etc. Classification label: "Confidential"

The default classification of any information that has not been formally classified is "Internal".

3.2.3 Security applications that have been installed on Information Systems (e.g. anti-virus, personal firewalls etc.) shall not be disabled and shall remain operational at all times, unless it has been disabled by IT administration for the purpose of installing software or a temporary workaround to fix another solution.

3.2.4 All files that are uploaded from external sources (via CD, USB memory devices, etc.) or downloaded from the Internet to Information Systems shall are scanned by anti-virus software before further use. A USB memory drive should only be used in a last case scenario, online methods of transfer should always be considered first.

3.2.5 Users shall be responsible for the security of any company information stored on portable media in their possession. Protection of such portable media, where possible, shall be by way of suitable encryption and/or strong passwords, or similar. Loss of such portable media (containing sensitive company data) shall be immediately reported the Executive Director and to IT Administration.

3.2.6 Unauthorised access, use, transmission, damage, deletion, suppression, alteration, or interference with SBC's Information Systems must not be undertaken.

3.2.7 Users shall not violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, the copying or distribution of "pirated" or other software products that are not appropriately licensed for use by SBC. Pirated content must never be downloaded, stored, or executed on Information Systems.

3.3 System and Network Usage

3.3.1 Before use of Information Systems, Users shall authenticate themselves by providing a valid Username and password/passphrase. At the end of the working session, they shall logoff the Information System. If a system is left unattended, it should be locked to prevent unauthorized access and use. Users are responsible for ensuring the machine they are using is locked when they are left unattended.

3.3.2 Information System passwords/passphrases shall be kept secret and not shared with anyone else, including IT administration staff. IT administration will ask Users to change passwords if they feel at any time the security of a password has been compromised.

All Users are responsible for using a strong password on all information systems that should meet the following conditions: Strong passwords should be at least 12 characters, contain a mixture of characters, numbers, and symbols and be different don't use the same password again.

Email accounts must have a different password to everything else.

3.3.3 Users shall not modify or tamper with Information System hardware. Additionally, they shall not install any software (executable code) without prior approval from IT Administration.

3.3.4 Users, unless authorized as part of their duties, shall not engage in activities that may affect the integrity or availability of the network. Activities include, use of high usage activities at times that would impact others, scanning of IP addresses, network reconnaissance, sniffing, hacking etc.

3.4 Web Usage

3.4.1 Use of Information Systems to carry out Internet browsing, electronic posting or publishing is acceptable, provided that:

a. it is carried out in a professional and responsible manner.

b. it does not otherwise violate SBC's policy or is detrimental to SBC's best interests.

c. it does not interfere with a User's regular work duties.

3.4.2 Electronic posting or publishing by Users on the Internet, public mailing lists, newsgroups, discussion groups, forums, blogs, etc. using SBC's credentials (e.g. official email address, official designation/ address) must contain a disclaimer stating that the opinions expressed are strictly their own personal opinions/beliefs and not necessarily those of SBC. SBC's trademarks, logos, branding, and any other SBC intellectual property shall not be used in connection with any personal electronic posts or publishing. This provision does not affect officially authorised postings on behalf of SBC.

3.4.3 Users must not make any discriminatory, disparaging, defamatory or harassing comments in their electronic postings or publishing.

3.4.4 Users, as per their employment contract, must not reveal any proprietary information, procurement details or any other material classified by SBC as Internal, Restricted or Confidential in their electronic postings or publishing.

3.5 Email, Messaging and Communications Activities

3.5.1 Users should not open email attachments received from unknown senders, as they may contain viruses, email bomb, malicious codes etc. Any email with an executable attachment should not be opened.

3.5.2 Users shall not use company email/messaging to distribute material that:

a. Is illegal or violates the morals and values of the church.

b. May offend an individual or a group of individuals.

c. Typically qualifies as unsolicited email, chain emails.

3.5.3 All emails sent externally shall have the following disclaimer attached:

"A company limited by guarantee. Registered in England and Wales

Company Number: 7605036 | Registered Charity Number: 1150563 | Registered Office: Stopsley Baptist Church, St Thomas's Road, Luton, LU2 7XP

NOTICE AND DISCLAIMER:

This email (including attachments) is confidential. If you have received this email in error, please notify the sender immediately and delete this email from your system without copying or disseminating it or placing any reliance upon its contents. We cannot accept liability for any breaches of confidence arising through use of email. Any opinions expressed in this email (including attachments) are those of the author and do not necessarily reflect our opinions. We will not accept responsibility for any commitments made by our Users outside the scope of our organisation. We do not warrant the accuracy or completeness of such information."

3.5.4 Users shall not send externally any information classified as Restricted, by email or similar, unprotected. Information classified as Confidential should be protected when sent internally or externally, by email or similar. Protection may be by way of suitable encryption and/or strong passwords, or similar. In most circumstances Users should use Google Drive to distribute files ensuring that information classified as restricted, internal, or confidential is only shared with the intended User. It is the responsibility of the User to ensure they do not put restricted, or confidential information in shared folders.

When a User emails contacts outside of SBC (stopsley.net) BCC must be used in all circumstances unless all parties have specifically agreed for their email addresses to be shared. In the event of a mistake this must be reported to the Executive Director immediately and they will decide if any further action should be taken.

Do not give out any database information over the phone or via email. Make sure both parties give permission for their data to be used.

3.6 Communication and Young People

A User's role description will include an acknowledgement and approval of technologies such as email, social networking, and mobile phone communications as a legitimate means of communicating with young people. It should also include the expectations of Stopsley Baptist Church in relation to their use. Parents will always be asked to give written consent before young people are sent electronic communications - this may be via the use of an online form or document or paper form.

Young people also need to be aware of the protocols that Users follow in relation to electronic communications. It is important to remember that as well as the parent/carer, young people over the age of 16 have a right to decide whether they want a User to have their contact details and should not be pressurised to provide them.

It is not appropriate to use these communication methods with children aged 11 years and younger.

Any data or forms taken at events should not leave either building unless taken by an authorized staff member / volunteer from building to building.

Forms should only be taken home with prior knowledge of the users line manager and their line manager should be notified when documents are returned – where possible electronic methods of storing data should be used.

3.6.1 Email

Email should be limited to sharing generic information, for example, to remind young people about meetings. If email is being used, Users will ensure that they are accountable by copying each message to a designated, agreed email address- e.g. safeguarding@stopsley.net. It is important Users use clear and unambiguous language to reduce the risk of misinterpretation, for example, avoiding inappropriate terms such as 'love' when ending an email.

3.6.2 Mobile Phones

Users need to take care in using mobile phones to communicate with young people:

- Mobile phone use should primarily be for the purposes of information sharing.
- Users should keep a log of significant conversations/texts.
- Any texts or conversations that raise concerns should be passed on to the User's supervisor or Designated Person for Safeguarding (DPS).

- Users should use clear language and should not use abbreviations like 'lol' which could mean 'laugh out loud' or 'lots of love'.

3.6.3 Social Networking

- Users should use SBC provided resources. For youth work the use of the closed Facebook group for parents. For children's work the use of MailChimp.
- The SBC Facebook pages should be used for broader public information.
- Database mailings should be used in any other scenario.
- Users should not send private messages to children on social networks. Users should ensure that all communications are transparent and open to scrutiny.
- Users should not accept 'friend' or 'following' requests from children on their personal site, nor seek to be 'friends' or a 'follower' of any child known to them in a church context.

3.6.4 Taking Videos and Photographs of Children

Since the introduction of the Data Protection Act in 1998, churches must be very careful if they use still or moving images of clearly identifiable people. There are several issues to be aware of:

- Permission must be obtained, via a written consent form, of all children who will appear in a photograph or video before the photograph is taken or footage recorded.
- It must be made clear why that person's image is being used, what it will be used for, and who might want to look at the pictures.
- If images are being taken at an event attended by large crowds, such as a sports event, this is regarded as a public area and permission from a crowd is not necessary.
- Many uses of photographs are not covered by the Data Protection Act 1998, including all photographs and video recordings made for personal use, such as a parent/carer taking photographs at school sports days or videoing a church nativity play.
- Children and young people under the age of 18 should not be identified by surname or other personal details, including email, postal address, or telephone number.
- When using photographs of children and young people, it is preferable to use group pictures.

3.7 Mobile Devices and Laptops

3.6.1 As mobile devices and laptops are especially vulnerable to theft and loss, stored data related to SBC shall be encrypted, wherever technically feasible. In case of theft or loss, the incident must be immediately reported to IT Administration as a security incident.

3.6.3 Mobile devices and laptops not directly owned or controlled by SBC shall not be used in conjunction with any Information System. Exemptions MAY be granted on a case-by-case basis; the User's line manager and IT Administration shall authorize these.

3.6.4 Mobile devices and laptops not owned or managed by SBC may be temporarily connected to SBC's networks provided they connect through approved channels.

3.8 Physical Security

3.7.1 Users shall be provided with an access card/code to permit access to SBC or GH's premises.

3.7.2. Users shall use only their own card to access premises. Sharing of cards is not permitted. New codes/access provided on a case-by-case basis authorised by Executive Director.

3.9 Incident Response

3.8.1 An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices or loss of service. All Users SHALL report any observed incident immediately to the IT Administration via email: chris.young@stopsley.net

3.10 Unacceptable Use

The following activities are, in general, prohibited:

3.9.1. Users shall not engage in any activity that is illegal, or outside the policies of the church, using Information Systems.

3.9.2 The following activities are strictly prohibited, with no exceptions:

a. Using Information Systems to actively engage in procuring or transmitting material that shall be deemed as obscene, to the church, or co-Users.

b. Making fraudulent offers of products, items, or services originating from any SBC account.

c. Circumventing the security systems implemented to protect Information Systems.

d. Providing SBC's Internal, Restricted or Confidential information including, personal information of SBC Users, its financial information, strategic plans etc. to parties outside SBC for personal gain.

e. Using of anonymous, faked, or forged identities on Information Systems.

4 Enforcement

Any Users found to have violated this policy may be subject to disciplinary action as per SBC's Staff Manual. This could include formal reprimands up to and including termination of employment. Criminal activities may be forwarded to appropriate law enforcement authorities within the UK.

5 Other Services

5.1 CCTV

- CCTV is shown on screens in both SBC and GH in locked offices where possible and is viewed by staff members and volunteers for the protection of themselves and others.
- Only specific individuals have access to the recordings of the CCTV and only shared at the discretion of the Executive Director.
- Remote access is usually not allowed, approved on a case-by-case basis by the Executive Director.
- The CCTV must not be tampered with by any personnel including service engineers without approval from IT Administration and Executive Director.
- Any camera faults should be reported as soon as practically possible.

5.2 Working From Home

Devices are provided for colleagues who may need to work from home.

Devices must be used with the same guidelines as when in the office.

When devices are being used at home authorised individuals may be able to track some usage. Company provided computers or mobiles should not be used for dealing with extremely sensitive personal data such as online banking.

5.3 Stopsley.net

Stopsley.net emails should be used for work use only.
SBC Shared areas should be used for their specific functions and personal files should not be placed there. Files that are to be shared outside SBC should be stored in the SBC Shared folder only. Due care should be taken when adding files to shared areas ensuring personal data is shared with correct personnel.

5.4 Network Devices

Network devices including but not limited to virgin media router, Wi-Fi access points, print server, network switch, point to point link, CCTV should not be rebooted or tampered with without authorisation from the IT Administrator or in their absence the Executive Director

5.5 Card Machines

The Sumup wireless card machine should only be used by trained and authorised personnel. The card machine must be checked out from the office and checked in after use. Payments must be logged with a pre-agreed code provided by Finance Manager or IT Administrator. Training for the card machine must only be provided by the IT Administrator. The card machines whereabouts should be logged. Any

declined payments should have a noted time and date, and this should be cross checked with the monthly reports which are sent to IT Administrator and Finance Manager.

5.6 BYOD (Bring Your Own Device)

In some cases, it may be necessary for staff to use their own devices to carry out their duty. They should ensure that any device used is up to date with the latest security updates. Any confidential information should be always stored safely and in line with GDPR regulations.

Conditions of BYOD include but are not limited to:

- Screensaver start at 5 minutes
- Device must have a strong password
- Agree storage of company information on that device

Any User's using their own device should be recorded in a register. Authorisation of a User BYOD device will be undertaken by IT Administration or the Executive Director.

5.7 Monitoring Internet Usage

To protect all Users of the church any devices connected to the networks at both SBC and The GreenHouse have their internet usage tracked. Traffic to the following sites within these categories is blocked: Adware, Dating, Nudity, Pornography, Web Spam, Alcohol, Drugs, Gambling, Lingerie/Bikini, Sexuality, Advertisements, Hate/Discrimination, Proxy/Anonymizer, Tasteless, Weapons.

This tracking and block were implemented in May 2021 when SBC and the GH started offering Guest WiFi throughout both buildings and in the neighbouring Community Garden. Tracking data is anonymous and is only visible to the IT Administrator who can see which blocked websites requests were made for but not which devices they came from.

6 GreenHouse Mentoring

6.1 GHM

- WhatsApp Control Groups (WCG) should be used within GHM to allow communication between relevant parties. This can include mentor/parents/carer/staff member. Messages should be relevant to GHM and mentee only. No messages should be sent outside the hours of 8am-8pm, except in exceptional circumstances through consultation with the GHM Manager. Users should not reply to messages outside of these times.
- Any agreed email communication must be copied to ghm@stopsley.net so there is a central record.

6.2 GHM Database

- Access to the GHM database will be granted on a case-by-case basis by the GHM Manager.
- Users must always make sure that the use of the database is not abused and used for legitimate purposes only.
- The database should not be tampered with and only used by competent Users.
- Database training will be provided by the IT Administrator or the GHM Manager.

6.3 GHM Website

- Users are granted the relevant access to the database by the IT Administator.
- The website will be the central point for the current training resources and all operational policies.

7 TeleMentoring

- Age limits for Social Media platforms will be observed at all times e.g. WhatsApp 16, Facebook 13 etc;
- Parental/ Guardian/ Carer (PGC) Consent must be explicitly given before a relationship can move to TeleMentoring;
- TeleMentoring should only be considered when all parties are happy to be involved. Mentors have the right to decide which tools they are prepared to use.
- Zoom and Whatsapp video are the only permitted TeleMentoring calling facilities.
- Volunteer/Mentor always will connect via PGC phone or device. PGC will then pass to Mentee. Volunteers will not ring a Mentee direct unless PGC has requested so and provided written consent beforehand.
- If Volunteer cannot get through to PGC, we recommend calling a maximum of 3 times. If unable to get through, then send a text via the WCG.
- If contacted via another number/ outside agreed time, then deny the call and let the PGC and Supervisor know.
- Volunteer profile, picture, screen name etc must always give families a professional and responsible impression.
- Users must always display their GHM badge whilst on video conferencing.
- Users video call is confidential with any young person. No other members of your household should participate or be visible or within hearing. Therefore, sit in a quiet area/ use headphones and NEVER show third parties in a call/ allow them to see the screen. Background – the camera should remain in a fixed location, with only the Volunteer in view. GHM can provide Zoom background pictures If required or you may use the Zoom standard "Blur" picture.
- Transcripts of Chat dialogues should not be saved without specific consent.

- Photographs – do not send images of yourself or accept ones of the Mentee.
- Never post pictures of young people or record video sessions.
- Never share contact details.
- Every meeting will also have a GHM member of staff present as a supervisor.
- When Users are participating with video, Users should take part in a quiet but communal area of their home. Preferably, the Mentee should not take part in the video call alone from their bedroom.

7.1 Group Video Conferencing (VC) Sessions Ground Rules

- There are some ground rules which should be explained at the beginning of the session and must be followed:
    - All group meetings should have at least a Host and Co-host.
    - Hopefully all will feel comfortable joining with video, however you may join with audio only if you prefer.
    - You should make sure an adult at home knows you are on a VC call (adults should not join in).
    - You should never record or take photos of your screen during a VC call.
    - You should not share the VC invite link with anyone else.
    - You should dress appropriately for the VC call (no pyjamas). GHM Mentors should wear their GHM Id Badges.
    - Be respectful of each other at all times – only write on the chat feature when requested to do so and avoid hurtful or rude comments.

7.2 Zoom Safeguarding Tips

- Don't fall for fake Zoom apps - Use Zoom's official website — zoom.us — to download Zoom safely
- Don't use social media to share conference links
- Protect every meeting with a password – do not share over social media
- Enable Waiting Room
- Pay attention to screen-sharing features - Limit screen-sharing ability to the host only initially, extend it to others during the call if required

8 Security Breach

8.1 Protocol

- In the event of a data breach or compromised system, IT Administration and Executive Director must be notified as soon as physically possible. All Users will have an out of hours contact number to do this.
- The Executive Director will decide the next steps to take depending on the severity of the incident.