IT Policy for SBC

Mar 2026

Church : Southwell Baptist Church
Approved by: Interim Steering Group
Effective Date: 01 March 2026
Review Cycle: Annual

---

1. Purpose

This policy sets out how Southwell Baptist Church (SBC) uses and protects information technology systems, data, and digital communications. It ensures:

- Protection of personal data
- Safe use of technology by staff, volunteers, and church members
- Compliance with UK law and charity regulations
- Safeguarding of children and vulnerable adults
- Responsible use of church IT resources

2. Scope

This policy applies to:

- Staff and ministers
- Volunteers and ministry leaders
- Trustees
- Contractors and third parties
- Anyone using church IT systems, devices, or data

It covers:

- Church computers and devices
- Email and cloud systems
- Website and social media
- Church management software
- Audio-visual systems
- Personal devices used for church work (BYOD)

3. Legal & Regulatory Compliance

The church will comply with:

- UK GDPR & Data Protection Act 2018
- Safeguarding legislation and guidance
- Charity Commission guidance
- Copyright, Designs and Patents Act 1988
- Licensing laws for music and media (e.g., Christian Copyright Licensing International and PRS for Music)

IT Policy for SBC

4. Acceptable Use of IT

Church IT systems must be used:

✓ For church ministry, administration, and mission
✓ In ways consistent with Christian values
✓ Respectfully and legally

Users must NOT:

✗ Access inappropriate or illegal material
✗ Use systems for personal business or political campaigning
✗ Install unauthorised software
✗ Share login details
✗ Send offensive, discriminatory, or harmful content

5. Data Protection & Privacy

5.1 Personal Data

The church collects and stores personal information for:

- Membership records
- Pastoral care
- Safeguarding records
- Gift Aid and donations
- Event registrations
- Volunteer management

5.2 Data Protection Principles

We ensure data is:

- Used lawfully, fairly, and transparently
- Collected for specific purposes
- Kept accurate and up to date
- Stored securely
- Retained only as long as necessary

5.3 Consent

Consent must be obtained before:

- Sending newsletters or marketing emails
- Publishing photos or videos
- Sharing contact details

—

IT Policy for SBC

6. Security Measures

6.1 Passwords

- Use strong passwords (minimum 12 characters)
- Enable multi-factor authentication where possible
- Never share passwords

6.2 Devices

- Keep devices updated and protected with antivirus software
- Lock devices when unattended
- Report lost or stolen devices immediately

6.3 Data Storage

- Store sensitive data only in approved systems
- Avoid storing personal data on USB drives or personal laptops
- Use encrypted cloud storage where possible

7. Email & Communication

Church email must be used responsibly:

- Avoid sharing sensitive personal data via email unless necessary
- Use BCC when emailing groups
- Beware of phishing scams and suspicious links
- Maintain a respectful and pastoral tone

8. Safeguarding & Online Safety

All online activities involving children or vulnerable adults must:

- Follow the church safeguarding policy
- Include parental/guardian consent where appropriate
- Use approved communication channels
- Avoid private messaging between leaders and minors
- Maintain transparency and accountability

9. Social Media & Website Use

Only authorised individuals may post on official church platforms.

Content must:

- Reflect Christian values and the church's mission
- Protect privacy and dignity
- Avoid posting personal details without consent
- Be respectful and non-political

IT Policy for SBC

Photos and videos require appropriate permissions.

10. Copyright & Media Use

The church will:

- Use licensed music, videos, and images
- Credit creators where required
- Ensure streaming and projection licences are current
- Avoid downloading or sharing copyrighted content illegally

11. Bring Your Own Device (BYOD)

Personal devices used for church purposes must:

- Be password protected
- Be kept updated
- Not store sensitive data permanently
- Be secured if lost or stolen

12. Incident Reporting

Report immediately:

- Data breaches
- Lost devices containing personal data
- Suspicious emails or cyber threats
- Safeguarding concerns related to digital communication

Reports should be made to the Church Administrator, Safeguarding Officer, or Trustees.

13. Training & Awareness

The church will provide appropriate guidance on:

- Data protection
- Safeguarding online
- Cybersecurity awareness
- Safe social media use

14. Policy Breaches

Failure to follow this policy may result in:

- Removal of system access
- Volunteer role review
- Disciplinary action
- Legal reporting if required

15. Review

This policy will be reviewed annually or when legal or operational changes require updates