

Cyber Security Guidance for Local Churches

Local churches hold valuable information, including membership records, safeguarding information, financial data, payroll records, donor details, and online banking access. Cyber criminals increasingly target charities, faith communities, and small organisations because they often have limited resources and volunteer-led administration. Churches should therefore treat cyber security as an essential part of good governance and stewardship.

Why Cyber Security Matters

A cyber incident can result in:

- Theft of church funds
- Loss of personal data
- Damage to reputation
- Disruption to worship, administration, and community services
- Breaches of GDPR and data protection requirements
- Loss of access to important records and documents through ransomware attacks.

Trustees and church leaders have a responsibility to take reasonable steps to protect church assets, including digital assets and information.

The 10 Essential Cyber Security Controls for Churches

1. Use strong passwords

Weak passwords remain one of the biggest causes of security breaches.

Good practice:

- Use three random words (for example: *IcelandLakePiano*)
- Never share passwords between staff or volunteers
- Use a different password for each system
- Consider using a password manager such as Microsoft Authenticator Password Manager, Bitwarden, or online/password-managers.

Government guidance:

National Cyber Security Centre (NCSC) Password Guidance:

<https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/password-managers>

2. Enable Multi-Factor Authentication (MFA)

MFA requires a second form of verification, such as a code sent to a mobile phone.

MFA should be enabled on:

- Microsoft 365 accounts
- Church email accounts
- Online banking
- Cloud storage
- Finance systems
- Social media accounts

Even if a password is stolen, MFA can often prevent unauthorized access.

Priority

If your church implements only one cyber security improvement this year, it should be MFA.

3. Keep Software Up to Date

Cyber criminals often exploit known vulnerabilities in outdated software.

Ensure that:

- Windows updates are enabled
- Mobile phones are updated regularly
- Antivirus definitions are current
- Church website software and plugins are patched
- Router firmware is updated

Automatic updates should be enabled wherever possible.

4. Back Up Critical Data

Churches should regularly back up:

- Membership databases
- Safeguarding records
- Financial records
- Payroll information
- Meeting minutes
- Governing documents
- Website content

Recommended approach

Follow the “3-2-1” principle:

- Keep three copies of important data
- Store them on two different media
- Keep one copy offsite or in the cloud

Government guidance:

<https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/always-back-up-your-most-important-data>

Test backups periodically to confirm they can be restored.

5. Protect Against Phishing

Phishing is the most common cyber-attack affecting organisations. Criminals send convincing emails, texts or messages designed to trick recipients into:

- Revealing passwords
- Transferring money
- Opening malicious attachments
- Clicking dangerous links

Common warning signs:

- Urgent requests
- Misspellings or unusual grammar
- Unexpected invoices
- Requests to change bank details
- Emails claiming to be from church leaders asking for gift cards or transfers

Remember

Always verify financial requests using a different communication channel.

Reporting phishing

Forward suspicious emails to: report@phishing.gov.uk

Guidance

<https://www.ncsc.gov.uk/collection/phishing-scams>

6. Secure Church Email

Church email accounts are frequently targeted.

Good practice

- Use Microsoft 365 or another reputable email provider
- Enable MFA
- Remove unused accounts promptly
- Never share login details
- Regularly review forwarding rules
- Use church email addresses rather than personal accounts for church business

Email compromise is one of the most common causes of financial fraud.

7. Protect Personal Data (GDPR)

Churches often process:

- Names and addresses
- Contact information
- Gift Aid records
- Volunteer information
- Safeguarding records
- Special category personal data

Access to sensitive information should be limited to those who genuinely need it.

Good practice:

- Encrypt laptops where possible
- Lock devices when unattended
- Store paper records securely
- Use BBC when emailing groups
- Remove information no longer required

ICO guidance:

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/>

8. Secure Devices Used by Staff and Volunteers

Church business is often conducted on personal devices.

Minimum requirements:

- Device PINs or passwords enabled
- Automatic screen lock enabled
- Devices updated regularly
- Trusted antivirus installed
- Ability to remotely erase lost devices

Do not store sensitive church information permanently on personal devices where it can be avoided.

9. Train Staff and Volunteers

Cyber security is not solely an IT issue. Everyone should know:

- How to identify phishing emails
- When to report suspicious activity
- Safe password practices
- How to protect personal information
- What to do if a device is lost or stolen.

Even a short annual awareness session can significantly reduce risk.

10. Have a Cyber Incident Response Plan

Churches should know what to do if:

- An email account is compromised
- Money is transferred fraudulently
- Data is stolen
- Ransomware encrypts files
- A church website is hacked

The plan should include:

- Who to contact
- How systems will be isolated
- Whether insurers need notifying
- When the ICO must be informed
- When trustees or elders should be informed
- How communications will be managed

Preparation significantly reduces the impact of a cyber incident.

Key Government Resources

National Cyber Security Centre (NCSC)

The NCSC is the UK's primary authority for cyber security guidance.

- Website: <https://www.ncsc.gov.uk>

Useful resources:

- Small Organisations Cyber Security Guide:
- <https://www.ncsc.gov.uk/collection/small-organisations-guide-to-cyber-security>
- Cyber Action Toolkit: <https://www.ncsc.gov.uk/cyberactiontoolkit>
- Phishing Advice: <https://www.ncsc.gov.uk/collection/phishing-scams>

Charity Commission

Guidance for trustees on managing cyber risks:

<https://www.gov.uk/guidance/protect-your-charity-from-cyber-crime>

Information Commissioner's Office (ICO)

- Data protection and breach reporting: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/>
- Personal data breach reporting: <https://ico.org.uk/for-organisations/report-a-breach/>

Action Fraud

- Report cyber-crime and fraud:
<https://www.actionfraud.police.uk>
Emergency cyber support: 0300 123 2040

Church Cyber Security Checklist

- ☐ Multi-factor authentication enabled
- ☐ Strong passwords in use
- ☐ Regular backups tested
- ☐ Software updates enabled
- ☐ Staff and volunteers trained
- ☐ Phishing reporting process established
- ☐ Data protection procedures in place
- ☐ Incident response plan documented
- ☐ Online banking protected
- ☐ Trustees regularly review cyber risks