

Social Media Safeguarding Guidelines

1. Reflect the Values of the Methodist Church

Your online presence allows you to shape how others see your church. Reflecting Methodist values ensures a positive, authentic image, strengthens outreach, and invites others into your church community.

The calling of the Methodist Church is to respond to the gospel of God's love in Christ and to live out its discipleship in worship and mission.

The Church exists to:

- Increase the awareness of God's presence and celebrate God's love (Worship).
- Help people to grow and learn as Christians, through mutual support and care (Learning and Caring).
- Be a good neighbour to everyone and in particular to people in need and to challenge injustice (Service).
- Make more followers of Jesus Christ (Evangelism).

2. Report Concerns Immediately

The safety and wellbeing of everyone, especially children, young people and vulnerable adults, must always be maintained in all digital activities undertaken on behalf of the church.

If you see, receive, or become aware of anything online that causes concern, including inappropriate messages, comments, images, videos, behaviour, or disclosures made through social media, email or messaging platforms, you must report this immediately. Concerns should be raised with the relevant Church Safeguarding Officer (local church, circuit or regional as appropriate). If you are unsure who this is, or if the concern involves that person, follow the Methodist Church safeguarding reporting procedures. Contact details can be found here: <https://www.methodist.org.uk/safeguarding/safeguarding-contacts/>

3. Account Access

Always ensure that accounts used to communicate on behalf of your church (Facebook, Instagram etc) have multiple administrators. This helps to ensure continuity if one individual is unavailable or leaves the church, and reduces the risk associated with accounts being controlled by a single person.

Administration access should only be given to individuals who have been safely recruited and authorised by the church. Anyone granted this access must be provided with clear written guidance outlining:

- The purpose of the account and who it represents
- Expectations around appropriate content, tone and conduct
- Safeguarding and data protection responsibilities
- How to handle concerns, complaints or safeguarding disclosures received online
- The circumstances under which access may be reviewed or removed




The **Methodist Church**

The calling of the Methodist Church is to respond to the gospel of God's
love in Christ and to live out its discipleship in worship and mission

Methodist Church House, 25 Tavistock Place, London WC1H 9SF | [methodist.org.uk](https://www.methodist.org.uk)

Registered charity no 1132208

The relevant Safer Recruitment documentation should be completed before administration access is granted. This should be accompanied by a 'Digital Key Holder' declaration, acknowledging that the individual understands their responsibilities and agrees to use the account only in line with church policies.¹ (Please see and access the Methodist Church guidelines on social media.)

Your church should maintain a written and regularly reviewed record of all individuals who have access to social media and digital communication accounts. This record should include:

- The name and role of each administrator
- The level of access granted
- The date access was provided and, where applicable, removed

Access should be reviewed at least annually, and immediately when someone steps down from a role or no longer requires access.

Digital Key Holder form included below.

4. Consent – Sharing Images Online

Do not take, use or share photographs or videos online of children, young people or vulnerable adults without appropriate written consent.

It may not be possible to gain written consent from every adult (photographs of a church congregation etc) in which case, it would be appropriate to let people know there will be photography happening for social media/ website.

Extra care should always be taken when capturing images in worship, groups, or events where children and young people are present.

Consent forms for using individuals in photographs and videos can be found here:
<https://www.methodist.org.uk/safeguarding/policies-procedure-and-information/forms/consent-forms-for-use-of-photography-and-video/>

5. Sharing Content

Don't share content in haste. Take time to consider carefully before sharing any content online on behalf of the church. Always read linked articles in full or watch videos to the end so that you clearly understand the message, context and tone of what you are sharing.

Do not share content that belongs to someone else (including images, videos, music or written material) unless you have permission to do so, or unless it is clearly stated that the content is free to share. Always credit the original creator where appropriate and follow copyright and licensing requirements.

When sharing content that includes personal information, images or identifiable details of individuals, ensure that this is done in line with UK GDPR and data protection legislation. Only share personal data where there is a clear lawful basis to do so, and never share private or sensitive information online.

Avoid sharing content impulsively or in response to strong emotions. If you are unsure about a post, pause and seek advice from another administrator or a church leader before sharing.

¹ <https://www.methodist.org.uk/for-churches/digital-church/digital-training-blog/creating-a-social-media-policy-for-your-church/>

6. Safer Recruitment

Any online platform, group or account set up for the purpose of communicating with or interacting with children and young people under the age of 18 must be managed in line with the Methodist Church's Safer Recruitment policy.

Individuals given administrator or moderation access to such platforms may require a current Enhanced DBS certificate /PVG. This applies whether the interaction takes place through social media, messaging apps, online groups, livestream chats or other digital platforms.

The requirement for employees or volunteers to carry out relevant criminal record checks are set out in legislation. Decisions on when and whether to undertake a DBS/PVG check are for the relevant employer or regulator to make based on what the law allows.

An Enhanced DBS certificate with access to the DBS Children's Barred List and a PVG with access to the Scottish barred lists for children and protected adults with access to the regulated activity, should be obtained when a role involves regulated activity with children.

In a digital setting this is set out as:

"Individuals who monitor the content of internet-based services aimed wholly or mainly for use by children on more than 3 days in a 30-day period. They must also:

- be able to access and remove content or prevent it from being published
- control who uses the service
- have contact with the children using the service"

The complete guidance can be found here:

https://assets.publishing.service.gov.uk/media/6687d04d899a6f92e5d9cd66/Child_workforce_guide.pdf

For Scotland <https://scottish-disclosures.co.uk/pvg-scheme/>

Before access is granted, safer recruitment processes must be followed, including:

- Completion of the appropriate Safer Recruitment forms
- Clear identification of the role and its responsibilities
- Verification that an Enhanced DBS with children's barred list or PVG is in place and up to date if necessary

A job description should be created for each role involving online contact with under 18s. This should clearly outline expectations, boundaries, safeguarding responsibilities, and lines of accountability.

No individual should be given responsibility for administering or moderating online spaces for children and young people until all safer recruitment requirements have been fully completed and recorded.

Examples of Digital Job descriptions included below

7. Maintaining Confidentiality

Sharing faith experiences, testimonies and stories online can be powerful, but must always be done with care, sensitivity and respect for confidentiality.

Before sharing any story, image or post that involves another person, always pause and ask: “Is this your story to share?” Even when information is shared with good intentions, posting it online without permission may breach trust, safeguarding principles, or data protection requirements.

Do not share any confidential, personal or sensitive information online without proper, informed permission. This includes details about someone’s personal circumstances, health, family situation, safeguarding matters, or pastoral conversations. Particular care must be taken where children, young people or vulnerable adults are involved.

Consent should be obtained before sharing testimony or stories involving other people. Consent can be withdrawn at any time, and churches should be prepared to remove content promptly if this happens.

If you are unsure whether something should be shared, do not post it. Seek advice from another administrator, church leadership or safeguarding officer.

8. Set Clear Boundaries

Clear and consistent boundaries must be maintained at all times in online communication. Church ministers, employees and volunteers must not engage or interact with children or young people under the age of 18 using their own personal social media or messaging accounts.

All online contact with under 18s should take place only through legitimate church platforms or accounts, which are appropriately monitored, accountable and managed in line with safeguarding guidance. This helps to protect children and young people, as well as adults, by ensuring transparency and reducing the risk of misunderstanding or inappropriate contact.

Private or one-to-one messaging with under 18s should be avoided wherever possible. Where one-to-one communication is necessary for pastoral or organisational reasons, it must follow Methodist safeguarding guidance, be appropriate, proportionate, and visible to others (for example, through shared accounts or copied-in oversight).

Adults should never:

- Use personal accounts to message under 18s
- Send private, secret or disappearing messages
- Communicate in ways that blur professional or pastoral boundaries

Account administrators should also set clear boundaries covering when accounts will be accessed, for example only during working hours, to protect their own wellbeing.

SAFEGUARDING FORM D (DIGITAL)

DIGITAL KEYHOLDER DECLARATION

Name of Church/ organisation:	
----------------------------------	--

Reason for digital access (role, responsibility, platform etc.):	
--	--

(e.g. social media admin, livestream operator, website editor, Zoom host)

Name of digital key holder:			
Address:		Phone No.:	
		Mobile No.:	
Post Code:		Email:	

Digital Access Details

Please list the platforms/systems you will have access to:

Social Media (e.g. Facebook, Instagram, X, TikTok):

Website / CMS:

Livestreaming Platforms:

Online Meeting Platforms (e.g. Zoom, Teams):

Cloud Storage / Shared Drives:

Other systems:

Declaration & Conditions of Digital Access

Before digital access is granted, you are required to agree to the following safeguarding conditions. These are designed to uphold the Methodist Church's commitment to safeguarding children, young people, and vulnerable adults in digital spaces.

Conditions of Issue

Account Security

I will keep all passwords, login credentials, and access codes secure.

Login details may be shared with appropriate person

No Unauthorised Access

I will not allow others to access accounts using my login.

I will not create additional users without permission of

Appropriate Use

I will ensure all content posted reflects the values and safeguarding policies of the Methodist Church.

I will not post, share, or engage with inappropriate, harmful, or unsafe content.

Safeguarding in Communication

I will avoid private or one-to-one messaging with children or vulnerable individuals unless explicitly authorised and in line with safeguarding policy.

I will ensure transparency in digital communication (e.g. copying in leaders, using group chats).

Online Meetings & Streaming

I will ensure appropriate moderation of online meetings (e.g. waiting rooms, muting, supervision).

I will not record sessions involving children or vulnerable adults without consent.

I will ensure appropriate content and behaviour during livestreams.

Content Management

I will ensure appropriate consent has been obtained before sharing images/videos of individuals.

I will remove any inappropriate or harmful comments or content promptly.

Data Protection

I will handle personal data in accordance with GDPR and Data Protection Act 2018.

I will not download, store, or share personal data unnecessarily.

Incident Reporting

I will report any safeguarding concerns, suspicious activity, or breaches immediately to the safeguarding officer or minister.

End of Role

I will relinquish all access immediately upon request or when my role ends.

I will not retain copies of data, passwords, or materials.

Suitability Declaration

I confirm that:

I have never been convicted or cautioned for any offence concerning children, young people, or vulnerable adults.

I understand my safeguarding responsibilities in digital environments.

Acceptance

I accept the above conditions of digital access.

Signed: _____

Date: _____

Authorised by (Church Representative): _____

Date: _____

Digital Access Issued

Platform/System Access Level Date Issued

Date to be reviewed



Privacy Notice (Digital Keyholders)

1. Why have I been given this notice?

You have been given this privacy notice because you have offered to act as a digital keyholder for **[insert name of church/organisation]**. The Methodist Church is committed to the protection of your rights under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This notice will inform you of your rights and provide information about how we hold and use your personal data.

2. What is personal data?

This is information, which indirectly or directly allows you to be identified via circumstances or specific details. It may include data such as names, addresses and dates of birth.

3. How do we process your data?

In compliance with the GDPR, the Methodist Church makes the following commitments about the processing of your data:

- Information will not be processed beyond what is necessary for the keyholder activities.
- Data about you will be kept up-to-date and records amended to address factual inaccuracies as soon as possible.
- We will store information securely, with the use of sufficient measures to protect your data from unauthorised access, loss or misuse.
- We will destroy data that is no longer required in a safe and appropriate manner.

We will use your personal data for the following purposes:

(Amend or add additional processing activities to fit individual circumstances)

- to maintain an electronic record of those who are willing to act as a digital keyholder for **[insert name of church/organisation]**, held by **[insert role of person maintaining record]**
- to inform you of information and updates that may be relevant to your role as a digital keyholder.
- To manage access to digital platforms
- To provide contact information where necessary for safeguarding or operational purpose.

4. What is the lawful basis for processing your personal data?

- Processing is necessary for the legitimate interests of the Methodist Church in Britain to enable you to undertake the role of digital keyholder within the Methodist Church in accordance with safeguarding policy and practice.
- Processing is carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided:
 - the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and
 - there is no disclosure to a third party without consent.

5. Sharing your personal data

Your data will be held in confidence and will be shared only where necessary with other members of the church or those engaging with church in order to facilitate the role and activities identified above. You will be informed if any further sharing of information is deemed necessary and your consent for this will be obtained, where appropriate.

6. How long do we keep your personal data?

Records of keyholder contact details will be retained for the period of their engagement in the role.

7. Your rights and your personal data

You have the following rights with respect to your personal data in relation to data held about you relating to safeguarding:

- the right to request a copy of your personal data which is held about you by the Methodist Church
- the right to request that the Methodist Church corrects any personal data if it is found to be inaccurate or out of date

- the right to request that the data controller provides you with your personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability), (where applicable)
- the right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing
- the right to object to the processing of personal data
- the right to lodge a complaint with the Information Commissioner's Office.

8. Additional Best Practice Guidance

Social Media

- Use official accounts only (no personal accounts for ministry communication)
- Avoid engaging in private pastoral conversations in public or unmonitored spaces

Livestreaming

- Clearly notify when recording/streaming is happening
- Ensure camera visibility is appropriate and safe

Online Meetings

- Use waiting rooms and passwords
- Ensure at least two responsible adults are present where children are involved

Cyber Security

- Use strong passwords and 2FA where possible
- Log out of shared devices
- Report hacking or suspicious activity immediately

Record Keeping

A copy of this agreement should be retained by:

The Digital Keyholder

The Local Church Council

9. Relevant Contacts

The Data Controller for all churches, circuits and districts is Trustees for Methodist Church Purposes which covers routine data processing activities.

For data processing relating to safeguarding, complaints and discipline the Data Controller is the Methodist Church in Britain. If you wish to make a subject access request concerning data held about you relating to safeguarding, complaints and discipline, it should be sent to the Data Protection Officer at dataprotection@methodistchurch.org.uk or

Data Protection
Methodist Church House
25 Tavistock Place,
London
WC1H 9SF

All other subject access requests should be sent to:

Trustees for Methodist Church Purposes

The Hive

47 Lever Street

Manchester

M1 1FN

Tel: 0161 235 6770

Further information is available from the TMCP website: <https://www.tmc.org.uk>

If you have any queries about data processing for keyholders, please contact a local minister or safeguarding officer.

Role Descriptions for Digital/Online Safeguarding

Social Media Administrator

Purpose of the Role

To support the church's mission and communication by managing and creating engaging, appropriate, and timely content for social media platforms.

Key Responsibilities

- Create and schedule posts promoting services, events, ministries, and encouragements.
- Maintain consistent branding, tone, and messaging across platforms.
- Respond to comments/messages where appropriate, directing enquiries to staff teams.
- Monitor engagement and suggest ideas to improve communication.
- Ensure content aligns with safeguarding, confidentiality, and church policies.

Role Requirements

- Confident using Facebook, Instagram, YouTube, etc.
- Good communication and creative skills.
- Ability to work as part of a wider communications team.
- Understanding of good boundaries when posting online.

Time Commitment

Approx. 1–2 hours per week, flexible. May involve occasional attendance at key church events.

Safeguarding / Data Boundaries

- Adhere to data protection rules, especially regarding photos and personal data.
- Ensure public-facing content is appropriate and safe.
- Do not post personal details, images of children, or sensitive information without appropriate consent.
- Follow church photography and online safety policies.

Who You Report To

Website Administrator (Volunteer)

Purpose of the Role

To keep the church website up-to-date, accessible, and helpful for newcomers and regular members.

Key Responsibilities

- Update content: events, ministries, sermons, staff details, notices, etc.
- Ensure links, forms, and menus function correctly.
- Upload sermons, images, and documents.
- Suggest ways to improve usability and layout.
- Maintain accuracy and remove outdated information promptly.

Role Requirements

- Basic experience with website Content Management System CMS (WordPress, Wix, Squarespace etc.).
- Good written English and attention to detail.
- Ability to follow branding and communication guidance.

Time Commitment

1–2 hours per week, flexible.

Safeguarding / Data Boundaries

- Adhere to data protection regulations, especially regarding photos and personal data.
- Ensure public-facing content is appropriate and safe.
- Do not post personal details, images of children, or sensitive information without appropriate consent.
- Follow church photography and online safety policies.

Reports To

Digital Content Creator (Volunteer)

Purpose of the Role

To produce creative visual digital content that supports the church's communication and outreach.

Key Responsibilities

- Design graphics for social media, events, and ministries.
- Create short videos, reels, or sermon clips.
- Edit video/photos as required.
- Work with staff to ensure content meets branding guidelines.

Role Requirements

- Familiarity with Canva, Adobe tools, or similar.
- Creativity and a strong eye for design.
- Ability to work to deadlines.

Time Commitment

Flexible, depending on project workload.

Safeguarding / Data Boundaries

- Do not use images of children without consent
- Keep raw footage secure and delete when no longer needed.
- Adhere to data protection regulations especially regarding photos and personal data.
- Ensure public-facing content is appropriate and safe.
- Follow church photography and online safety policies.

Reports To

Photography & Videography (Volunteer)

Purpose of the Role

To capture high-quality images and videos of church life for use in communications and outreach.

Key Responsibilities

- Attend services and events to take photos/videos.
- Edit and prepare media for web and social media use.
- Store files securely in church systems.
- Work with ministry leaders to capture appropriate moments.

Role Requirements

- Basic photography/videography skills.
- Ability to take natural, respectful images in church settings.
- Awareness of consent and privacy requirements.

Time Commitment

Varies depending on events.

Safeguarding / Data Boundaries

- Strictly follow church photography policy.
- Never photograph children without explicit written consent.

Reports To

Digital Ministry Coordinator *Leadership Role* (Volunteer)

Purpose of the Role

To oversee, organise, and support the full digital and technical ministry team.

Key Responsibilities

- Recruit, train, and care for volunteers across digital teams.
- Create service rotas and ensure coverage for events.
- Maintain standards across sound, media, livestream, and online content.
- Liaise with church leadership to align digital communications with church vision.
- Manage equipment checks and maintenance planning.

Role Requirements

- Strong organisation and communication skills.
- Ability to lead volunteers kindly and effectively.
- Good understanding of digital ministry areas.
- Problem-solving and calm under pressure.

Time Commitment

Regular weekly involvement + Sundays + planning time.

Safeguarding / Data Boundaries

- Model high standards in confidentiality and online safety.
- Ensure volunteers follow good practice.
- Adhere to data protection regulations, especially regarding photos and personal data.
- Ensure public-facing content is appropriate and safe.
- Do not post personal details, images of children, or sensitive information without appropriate consent.
- Follow church photography and online safety policies.

Reports To

Optional ones, that may not be to do with digital safeguarding, will let you make the decision

IT Support (Volunteer)

Purpose of the Role

To ensure church staff and volunteers can use their technology effectively and safely.

Key Responsibilities

- Provide basic troubleshooting for computers, printers, and software.
- Assist with setting up new devices.
- Support with Wi-Fi and network issues.
- Document recurring issues and escalate where needed.

Role Requirements

- General IT knowledge.
- Problem-solving skills.
- Patience and good communication.

Time Commitment

Flexible, on-call or ad-hoc.

Safeguarding / Data Boundaries

- Do not access personal files without explicit permission.
- Maintain confidentiality at all times.

Reports To

Livestream Operator (Volunteer)

Purpose of the Role

To provide high-quality livestreams of services, enabling online participation for those unable to attend in person.

Key Responsibilities

- Set up cameras, microphones, streaming software, and online platforms. (If needed/not already set up)
- Operate livestream during services, adjusting audio/video as needed.

- Troubleshoot technical issues calmly.
- Upload service recordings and ensure correct naming/storage.
- Keep equipment tidy and stored safely.

Role Requirements

- Basic technical competence.
- Ability to focus for extended periods during services.
- Calm under pressure.

Time Commitment

During Sunday services + occasional special events.

Safeguarding / Data Boundaries

- Ensure cameras avoid children where required.
- Follow guidance on which parts of the service may be streamed.
- Adhere to data protection regulations, especially regarding photos and personal data.
- Do not post personal details, images of children, or sensitive information without appropriate consent.
- Follow church photography and online safety policies.

Reports To

Sound Technician (Volunteer Role)

Purpose of the Role

To ensure clear, balanced audio for worship, teaching, and livestreams.

Key Responsibilities

- Set up microphones, monitors, and sound desk before services.
- Mix live sound throughout the service.
- Coordinate with worship leaders, speakers, and livestream team.
- Pack down and store equipment safely.
- Identify and report equipment issues.

Role Requirements

- Good ear for sound balance.
- Reliability and attention to detail.
- Willingness to learn sound desk operation.

Time Commitment

Sunday services + practice sessions and occasional events.

Safeguarding / Data Boundaries

- Avoid handling personal data or equipment unnecessarily.
- Follow safeguarding protocols when interacting with under-18s.

Reports To**Presentation & Media Operator (Volunteer)****Purpose of the Role**

To support worship and teaching by running visual media (lyrics, Bible verses, notices, videos).

Key Responsibilities

- Prepare service slides in EasyWorship/ProPresenter/PowerPoint.
- Operate slides during services in coordination with worship leader and preacher.
- Ensure accuracy and smooth transitions.
- Test videos and media before the service.

Role Requirements

- Competence with computers and presentation software.
- Good timing and concentration.
- Ability to work as part of a team.

Time Commitment

Sunday services + preparation time.

Safeguarding / Data Boundaries

- Ensure slides do not contain personal details without consent.
- Maintain confidentiality when handling internal documents.

Reports To

Fiona Fidgin, Digital Communications Officer
April 26