Digital Safeguarding Best Practice Reference Document

A detailed list of FAQs that help unpack Methodist safeguarding policy in an online context, including resources to help with practical application of this guidance. This is an evolving and interactive document, and not a comprehensive list. You can click highlighted links to navigate the document and find additional external resources.

This is a long document, and not intended to be read cover to cover - it will hopefully answer a specific question you have, and is a resource you may want to keep revisiting. If you are looking to get an overview and general understanding you may want to skim through the "short answers" and look at the first FAQ in each section.

The contents of this document have been created by Katy Spencer-Madden (previous District Safeguarding Officer) and Elliot Crippen (District Digital Enabler).

Key:
Should - recommended best practice by us
Must - compulsory practice to comply with safeguarding policies, GDPR, or other legal obligations

The majority of this document deals with online safeguarding relating to traditional church structures. If you have questions relating to pioneer ministry or fully online church communities or initiatives that don't have traditional church governance and oversight then do get in touch with us.

For further information relating to Safeguarding or Digital, see the Yorkshire North and East District website:
www.yorkshirenemethodist.org/our-work/safeguarding
www.yorkshirenemethodist.org/digital-resources

Contents- what are you looking for?

Click on the links below, or in the "outline" panel on the left, to jump to a section:

Zoom & Video Conferencing

- How to distinguish between a church-run Zoom meeting and a meeting set up in a personal capacity by a sub-group or group of friends in the church?
- Should password holders of church Zoom accounts and/or 'hosts' of Zoom meetings have a DBS check, and/or have undertaken the Methodist safeguarding training?
- What is best practice for using the chat function in Zoom?
- Can you have a Zoom meeting that contains a mix of under 18s and adults?
- Should you share Church Zoom links online?
- Do you need verbal or written permission to record a Zoom meeting to publish online?
- Best practice guidance for those attending a zoom meeting

WhatsApp

- How to distinguish between a church-run WhatsApp group chat and a chat set up in a personal capacity by a sub-group or group of friends in the church?
- Should WhatApp Group admins have a DBS check, and/or have undertaken the Methodist safeguarding training?
- What is best practice for adding people to a church WhatsApp group chat?
- What group rules or code of conduct should you have in a church WhatsApp group?
- Can a church WhatsApp group contain a mix of under 18s and adults?

Church Websites

- Should editors of Church Websites have a DBS check, and/or have undertaken the Methodist safeguarding training?
- Should photos/videos of identifiable under 18s posted online in the past without correct permissions, sometimes having been online for many years already, be removed?
- Best practices for accessing websites through church public Wi-Fi

Individual Social Media Use

- Should you create a seperate 'work' social media account as a minister, lay employee, or volunteer?
- What is best practice guidance for using social media in a personal capacity as an employee, minister, volunteer, or in a leadership position?
- Can under 18s who have a role in the church / leadership position be friends with other under 18s, or would they need to unfriend all their peers?
- What should you do if you come across young people in your church under 13 who have social media accounts?
- How do we safeguard people from 'auto play' videos?

Youth Groups, Children & Young People

- What are the best practices for leaders communicating with under 18s via electronic means?
- What consent and consent forms are needed to include identifiable under 18s in church videos, photos, audio, or live streams that will be used online?
- What is best practice guidance around church youth Facebook Groups?
- What are the best practices for hosting a Zoom youth group or meeting for under 18 year olds?
- What is best practice for youth groups or young leaders using TikTok in an official capacity?
- Signposted links for online safety for parents and children

Church Social Media Accounts

This section is for any official Methodist organisation accounts on Facebook (using Pages), YouTube, Twitter, and/or Instagram. Where "church social media account" is used, this should also be taken to mean any circuit, district, youth group, or other official Methodist social media account, whether local, regional, or national in nature.

General advice on how to use Social Media for churches:
District Digital Resources Hub (Yorkshire North and East Methodist District)

---

1. **Should admins and password holders of church social media accounts have a DBS check, and/or have undertaken the Methodist safeguarding training?**

Short answer: Admins of social media accounts aimed at children (under 18s) must have a children's worker (unregulated) DBS check. However, those with access to church-run social media accounts (not predominantly aimed at under 18s), whether employed or volunteers, don't need a DBS but should have been safer recruited: (a single all-in-one form is provided below that covers *'digital key holder form', 'role description', 'self-declaration SD/4' and 'code of practice'*).

It is not a requirement for admins to do the Methodist Safeguarding Training (Foundation or Advanced) however we would suggest that all social media admins undertake specific training in the form of watching or reading our 'code of practice'

Resources:

- **Church Social Media Access Form** (created 2022)
  (all-in-one 'digital key holder form', 'role description', 'self-declaration' and 'code of conduct' to be signed by those with access to church social media accounts)

- Code of Conduct (an extract of the above document)

Longer explanation and other scenarios: being an admin of a church social media account (even if it's just holding the login details) is a role with the church, and all roles (employed or volunteer) need to follow the safer recruitment process. The only unique aspect to social media is the tailored 'code of practice' which is there in place of no existing training that is specific to this role. We would encourage all who currently hold roles that don't have the above in place to look at completing the safer recruitment process retrospectively as a matter of good practice (particularly the Church Social Media Access form). The safer recruitment process is also required of Facebook "Editors" (not just those who hold the specific "Admin" role on Facebook). Ministers are exempt from the safer recruitment process however we would recommend that they still fill in a Church Social Media Access form, detailing all the social media accounts they have access to. For lay employees, such as admin staff, who use church social media

accounts as part of their role but are not in a dedicated digital role, we would encourage giving consideration to whether any or all of the safer recruitment steps need to be done in addition to the process that was undertaken for their current role, with the recommendation that the Church Social Media Access form is filled in. If access to a church social media account is being given for a specific purpose in a time limited way (such as temporary access in order to use Facebook Live, gather viewing figures, or another one-off situation) then the full process doesn't need to be followed as long as the person is removed, or the password changed, after the specific purpose is complete. Safer recruitment to social media roles only needs to be done once, as it's common for employees and volunteers to be admins of multiple accounts, platforms, and for different churches. There is space on the Church Social Media Access form to list multiple social media accounts so the form only needs to be completed once.

[last updated Oct 2021]

---

2. **Can under 18s be admins of church social media accounts?**

Short answer: Admins of church social media accounts should be over 18 in age.

Longer explanation and other scenarios: where under 18s are admins or have access to church run social media accounts then they must be supervised in this role. On most social media platforms, all actions of the admins are visible to other admins, and so actions taken by an under 18 can be easily monitored and supervised. Where the under 18 is assisting due to a lack of digital skills amongst other staff or volunteers, there might need to be a proactive approach to logging in at semi-regular intervals to oversee the actions that the under 18 is taking on the account, particularly that posts and any private messages are in line with church expectations.

Where under 18s have set up their own social media accounts on behalf of a youth group, church friends, or other church related group, but it is not run or officially overseen by the church, then this is out of our control and it is not down to the church to moderate the account. Under 18s are welcome to set up or admin their own social media channels, some of which may relate or support church work, however these should ideally not contain the official name of the church, in order to avoid confusion about who is accountable and runs them.

[last updated Oct 2021]

---

3. **How many people need to hold the passwords or have admin access to church social media accounts?**

Short answer: Church social media accounts must have at least 2 admins or people with the login details, but ideally 2-3 people should have access, with the church or circuit office holding details as a back up.

Longer explanation and other scenarios: It is unsafe to have a social media account with only 1 admin or password holder, and this should be avoided, even if it means temporarily removing the social media account until a second admin is found. For churches where there is a larger team looking after social media, it is advised that different levels of access are granted (where the social media platform allows) - for example on Facebook most can be made "editors" with just 2-3 people holding admin status.

[last updated Oct 2021]

---

4. **Do admins of church social media accounts need to be church members, or include the minister or a church office holder?**

Short answer: If the safer recruitment process has been followed, including the access form detailed above in question 1, then there is an accountability to those holding this role and it is not necessary for it to be a requirement that admins are church members, or necessary for the minister or a church office holder to be part of the admin team.

Longer explanation and other scenarios: where there are existing church social media accounts with volunteers in admins roles without safer recruitment etc. then we would recommend that it may be good practice to have a church officer holder, member or minister as an admin, in order to safeguard the church (such as where someone moves on and the church lose access to the account)

[last updated Oct 2021]

---

5. **Should Churches on Facebook have a profile, page, or group?**

Short answer: Churches must not have a Profile, but can choose between a Page or a Group. Generally, a Page is used for external communication and reaching new people (like an interactive church website) and a Group is used for internal discussion, sharing, and discipleship (like a members only forum).

Longer explanation and other scenarios: It's easy to get confused between the three different options you have on Facebook. In simple terms, a 'profile' is for individuals, a 'page' is a public profile for businesses, charities or churches, and a 'group' is a community-based feature where small groups of people can communicate together.

A Facebook Profile is created when you set up an account on Facebook as an individual. If you're on Facebook yourself and have set up an account, then you have a Facebook Profile. In the words of Facebook: "A profile is a place on Facebook where you can share

information about yourself, such as your interests, photos, videos, current city and hometown. To see your profile, click or tap your name or profile picture at the top of Facebook." It is designed for individuals in mind – it's for one person, where you can add other people as friends, and can choose to share personal information such as gender, age, relationship status and more. Facebook accounts shouldn't be accessed by more than one person, and a personal profile shouldn't be passed from one person to another. As such they shouldn't be set up for a Church.

Note: under Facebook's Terms of Service you should only have one Facebook account as an individual and shouldn't create a second account for yourself for work purposes. Instead, for those who work with young / vulnerable people, you should adjust your personal privacy settings so only a small amount can be viewed publicly. You have complete control over what information is visible to others on Facebook and can restrict it as much you need (including not allowing others to add you as a friend).

Facebook Pages are great for Churches as we are an organisation that wants to connect with our 'customers' and communities – this is exactly what Facebook Pages are designed to facilitate. Facebook Pages give you many additional features you don't get with a personal profile. Multiple people can be given access to the Page and can be assigned 'roles' depending what they need to do. Think of your Facebook Page as the front porch of your church, it is the public face of your church and can be a useful addition (or alternative) to your website. In the words of Facebook: "You must have a profile to create a Page or help manage one. Pages are places on Facebook where artists, public figures, businesses, brands, organizations and non-profits can connect with their fans or customers. When someone likes or follows a Page on Facebook, they can start seeing updates from that Page in their News Feed."

A Facebook Group might be suitable for your church but remember that it is best used for internal communication. They are great for your congregation to communicate with each other during the week and promoting discipleship (e.g. you could have a group for your church house group, messy church, toddler group, youth group etc.) but they are not great for inviting visitors to join – as the process of having to ask to 'join' your church group is off putting and can give the impression that your church is an exclusive 'club'. How many of your existing congregation are already on Facebook? If lots are, then a church Facebook Group provides a space for building relationships and connecting through the week. If a Facebook Page is your front porch, then your Facebook Group is the living room. In the words of Facebook: "You must have a profile to create a group or help manage one. Groups are a place to communicate about shared interests with certain people. You can create a group for anything — your family reunion, your after-work sports team, your book club — and customize the group's privacy settings depending on who you want to be able to join and see the group. When you join a group on Facebook, you start seeing content from that group in your News Feed."

[last updated Oct 2021]

6. **Should Church Social Media accounts be private or public?**

Short answer: Official church accounts should be public to be most effective and there is no safeguarding reason why they should be made private.

Longer explanation and other scenarios: by default Facebook Pages are public and cannot be made private. Most other social media platforms, such as Instagram and Twitter, have options of public or private - however most have introduced more sophisticated privacy options, settings and features that allow for more selective application of safety measures. Platforms such as Snapchat are not recommended for church use, or use by those in leadership positions as part of their role. Platforms such as TikTok can be used, if best practice guidance is followed, however it is best utilised by pioneers and young leaders seeking to reach a new generation in an appropriate way. At the current time it is unlikely to be a useful platform for a Methodist Church, recognising it is still predominantly a platform for Gen Z (11-26 year olds at the time of writing) with it's own unique culture.

---

7. **Can Church Social Media accounts follow, comment, or interact online with under 18s, either on their posts or your own posts?**

Short answer: An official church or youth group account should take every effort not to follow anyone under 18, or like or comment on any posts they make. However, it is ok for a church account to respond to comments or interact in an appropriate way in a public space with an under 18 such as within the comments of a church post.

Longer explanation and other scenarios: We would not encourage Church accounts to follow or friend under 18s, however, if there is to be engagement with young people on social media, the best way would be public engagement via your church account (such as responding to public comments). Church accounts can respond to comments on their own posts from under 18s, as in many cases the age of the commenter won't be obvious or even accessible. If you are contacted directly on a church social media account by a known under 18, alert the other admin or account holder that this has happened in order to remain accountable. Do not engage in conversation beyond responding to simple queries.

[last updated Nov 2021]

---

8. **Do churches need to protect under 18s / vulnerable adults from being traceable when they follow or interact with a church social media account?**

Short answer: Churches should have a public social media account and it's not the church's responsibility to protect it's followers from being traceable

Longer explanation and other scenarios: Social media accounts (excluding closed spaces, like Facebook Groups, WhatsApp group chats etc.) are designed to be public. They are for external communication, much like a church website, and so best practice would be to make church Instagram and Twitter accounts public. It is not a church's responsibility to protect its followers from being visible online if they choose to engage with your church account, as this is controlled by individual users, not the church. On platforms like Instagram you cannot hide your list of followers on a public page. So the best way to safeguard under 18s and vulnerable adults who follow or interact with you on social media is to encourage them to personally use privacy settings to restrict access to their accounts. It's their choice, but it's good practice as an individual to consider having a private account (on the platforms that allow this) or using the extensive privacy settings on Facebook and Instagram to control what people can see and how they can interact with you.

Resources:

How to use Facebook privacy settings and tools

How to use Instagram privacy settings and tools

[last updated Jan 2022]

---

9. Should all churches / circuits / districts have a social media policy?

Short answer: This guidance document can be used as your social media policy, and you don't need to create your own. However we have provided below an example model social media policy which you can adopt in your local context.

Longer explanation and other scenarios: In most cases a social media policy is there to safeguard the church and employees by having clear written expectations of how social media admins (whether employed, volunteers, or ministers) will conduct themselves online, on church and personal accounts. If you are following Methodist Church safeguarding procedures (such as implementing safer recruitment as described in question 1) then it is not necessary for a church / circuit / district to have a separate social media policy. It is advisable that churches / circuits / districts follow this guidance document, which puts Methodist Safeguarding Policy into practice where it relates to social media. For example, much of what a social media policy normally covers is already dealt with in code of conduct attached to the "Social Media Access Form" for admins (see the resources section of question 1). As such it is not normally necessary to have a separate social media policy for your church / circuit / district. However, much like the way local churches adopt a 'model church safeguard policy' that allows us to take local ownership of the the national Methodist Church Safeguarding Policy, we have provided below a sample model social media policy. This provides some general overview of "what we are committed to", with links back to this guidance document for practical examples of how to implement this.

Resources:

- **Example Model Social Media Policy for Churches**

[last updated Jan 2022]

---

10. How should a church give access to its social media accounts?

Short answer: Each platform has its own method for adding additional admins and it's important to follow best practice to achieve this in a safe and professional way.

Longer explanation and other scenarios: see below for seperate social media platforms

Facebook:
The creator of the Facebook Page, or existing admins, can go to "settings" on the Facebook Page to add other personal profiles as admins. To become an admin in this way, you must already have a personal Facebook account. You shouldn't set up a separate 'work' Facebook account to use for this purpose, or have a single Facebook account as admin of the page that everyone logs-in with to access the page. Advanced option: for larger teams using Facebook Pages, or if admins don't want their personal profiles visible to other admins (admin profiles are never visible to the public), churches can use Meta Business Suite. This is a little more complicated but provides additional features and safeguarding measures for managing a team of admins (can also be used to grant access to connected Instagram accounts). How to manage page roles on a Facebook Page

Instagram:
The simplest route for Instagram is to provide staff and volunteers with the username and password for the church account (making sure to use the Social Media Access Form from question 1). However, as mentioned above, you can also give admins access to Instagram through a linked Facebook Page or Meta Business Suite.

Twitter:
Simply provide staff and volunteers with the username and password for the church account (making sure to use the Social Media Access Form from question 1)

YouTube:
It can be tempting to set up a church Gmail account for use with YouTube and give people the username and password, however, this isn't best practice. Logging in via someone else's Google account will give access to all linked applications, not just YouTube (search history, Gmail, Google Drive, calendar, Google Docs, account settings and more). This may not be an issue if you've set up a blank Google account, however, these products are not designed to be used in this way - for example Google may identify that multiple people are logging in from different devices and locations, and then require you to confirm your identity via a phone message (two-factor authentication). This can cause logistical issues every time you try to access the YouTube channel. Best practice is

to add people (via their personal Google account) as editors or managers of the YouTube channel via the YouTube Studio. To become an admin in this way, you must already have a personal Google account. This will give admin access without needing to login using different details (works very much the same as adding admins to Facebook Pages). Add or remove access to your YouTube channel

[last updated Jan 2022]

---

11. What consent do you need for photos and videos on social media?

See answer under the Consent Forms section

---

12. Should photos/videos of identifiable under 18s posted online in the past without correct permissions, sometimes having been online for many years already, be removed?

See answer under the Consent Forms section

---

13. What is best practice for using TikTok for your church or youth group?

See answer under question 14 of the Youth Groups, Children & Young People section

Church Facebook Groups

This section is specifically about the "groups" feature on Facebook, but could apply to other communal group spaces online. Where "Church Facebook Group" is used, this should also be taken to mean any circuit, district, youth group, or other official Methodist Facebook Group, whether local, regional, or national in nature.

---

1. Should Facebook Group admins have a DBS check, and/or have undertaken the Methodist safeguarding training? And have the same safer recruitment process as church social media account admins?

Short answer: for any official church / circuit / district run Facebook Group (or any Facebook Group set up or run by a Methodist organisation) all the same guidance applies

as was provided for church social media account admins (see question 1 from the church social media accounts section). However, if you're already recruited to an online role, such as admin of a church Facebook Page, then the Social Media Access form and other safer recruitment processes only need to be done once.

Longer explanation and other scenarios: Admins of Facebook Groups aimed at children (under 18s) must have a children's worker (unregulated) DBS check. However, those with access to church-run Facebook Groups (not predominantly aimed at under 18s), whether employed or volunteers, don't need a DBS but should have been safer recruited: (a single all-in-one form is provided below that covers *'digital key holder form', 'role description', 'self-declaration SD/4' and 'code of conduct'*). It is not a requirement for group admins to do the Methodist Safeguarding Training (Foundation or Advanced) however we would suggest that all Facebook Group admins undertake specific training in the form of watching or reading our 'code of practice'. Safer recruitment to social media roles only needs to be done once, as it's common for employees and volunteers to be admins of multiple accounts, platforms, and for different churches. There is space on the Church Social Media Access form to list multiple social media accounts so the form only needs to be completed once.

For more details and resources, see answer to question 1 in the 'Church Social Media Accounts' section

[last updated Jan 2022]

---

2. **What is the guidance around church youth Facebook Groups? (or any Methodist Facebook Group aimed at under 18s)**

See answer under the "Youth Groups, Children & Young People" section

---

3. **Can you have a Church Facebook Group that contains a mix of under 18s and adults?**

Short answer: Facebook Groups specifically for Youth Groups or under 18s should not contain adults who aren't youth group leaders or safer recruited. However, Church or general Facebook Groups could, in principal, contain a mix of under 18s and adults as long as the Facebook Group has good guidelines, rules, and moderating. The Church Social Media Accounts section details how Adults can communicate with under 18s in a public context, where appropriate, such as in the comments of a public post, and this is the same principle that applies to a Facebook Group. In this context all communication between the under and over 18 year olds is being monitored.

Longer explanation and other scenarios: See more guidance for Facebook Groups specifically for under 18s under the Youth Groups, Children & Young People section.

Church Facebook Groups must have at least 2 admins (or a Page as admin which has itself 2 or more admins), but ideally 2-3 people should have access (the larger the Faecbook Group, the more admins or moderators you might need). It is unsafe to have a Facebook Group with only 1 admin, and this should be avoided, even if it means temporarily removing the Group until a second admin is found. For churches where there is a larger team looking after social media, it is advised that different levels of access are granted (Facebook Groups provide two different levels of oversight: admin and moderator - info on the difference can be found here).

It is important to note that admins and moderators personal accounts will be the ones visible in the group when they post, so personal account privacy settings are very important. It doesn't matter who fulfils the role of admin in a group as long as they are over 18, and can be decided on a church by church basis. However, it is essential that they have been through the safer recruitment process (as outlined in question 1 of Church Social Media Accounts).

We would suggest that it is best practice for all Facebook Groups to have 'group rules' (either using the official 'group rules' feature on Facebook, or by displaying written groups rules within the group description or as a post in the group). See question 5 below for more details.

Admins and Moderators also have access to features such as turning off commenting on a post, turning on post approval for specific members, and removing members from the group. This external article explains this more and may be a good resource for church admins to read. We would encourage all group admins and moderators to familiarise themselves with these practical safety features.

See question 6 for more guidance on safely moderating a mixed Facebook Group.

[last updated July 2022]

---

4. Should church / circuit / district Facebook Groups be set to public or private?

Short answer: There's no right or wrong answer, as it will depend on context whether a public or private group is the best setting to safeguard those in the group. Groups that are specifically for under 18s should be made private.

Longer explanation and other scenarios: There are two privacy settings for Facebook groups: Public: anyone on or off Facebook can see who's in the group and what they post. Private: only members can see who's in the group and what they post.

A public group can be a good option where you don't want to create a barrier for entry, and all the content shared is safe to be in the public domain. Typically, a public church group can be easier to moderate, as there is an accountability to all the content and members of the group being public. Admins and moderators will need to make sure no

personal, confidencial, or sensitive information is shared without proper permission and compliance.

A closed group can be a good option where a secure safe space for sharing is needed, and all the content is only available to an approved group of people. This space is typically safer for vulunruble groups, and allows members to be more open and honest. Admins and moderators will need to monitor discussion more closely to ensure it is kept as a safe space, as more personal, confidencial and sensitive information is likely to be shared. Admins and moderators will also need to review membership requests to join the group.

[last updated Jan 2022]

---

5. Should all Church Facebook Groups have 'group rules'? And what are the best practice guidelines for these?

Short answer: We would suggest that it is best practice for all Facebook Groups to have 'group rules' (either using the official 'group rules' feature on Facebook, or by displaying written groups rules within the group description or as a post in the group). As with any other form of online socialising, the behaviour of the users play a big part in how safe the Facebook Group is. Cyberbullying, giving away personal information, inappropriate images or messages and peer pressure are universal issues that can pose a risk on any service.

Longer explanation and other scenarios: You can use the official group rules feature provided by Facebook to add up to 10 rules for your group. New groups can benefit from having rules to set expectations of the group culture early. Great rules tell members how they can engage with the group. Rules can help prevent conflict as your group grows and provide a feeling of safety for group members. The group rules feature offers four example rules that you can use immediately or edit. These example rules are based on some of the most common rules admins use across many types of groups:

- Be Kind and Courteous
  We're all in this together to create a welcoming environment. Let's treat everyone with respect. Healthy debates are natural, but kindness is required.
- No Hate Speech or Bullying
  Make sure everyone feels safe. Bullying of any kind isn't allowed, and degrading comments about things like race, religion, culture, sexual orientation, gender or identity will not be tolerated.
- No Promotions or Spam
  Give more than you take to this group. Self-promotion, spam and irrelevant links aren't allowed.
- Respect Everyone's Privacy
  Being part of this group requires mutual trust. Authentic, expressive discussions make

groups great, but may also be sensitive and private. What's shared in the group should stay in the group.

As well as these standard Facebook rules, we would also suggest some additional rules, where applicable. Here are some examples which you are welcome to use:

- Be transparent - Don't mislead people about who you are, or use pseudonyms.
- Disagree with love - Being a Christian means that sometimes we must speak out and challenge injustice. But remember there is a real, & possibly vulnerable, person at the receiving end of what you say.
- Be careful when sharing content - Don't share in haste. Read linked content thoroughly, or watch a video to the end so you know exactly what you are sharing before you judge whether it is suitable to share. Make sure you have permission for any photos you share, particularly containing under 18s.
- Maintain confidentiality - If telling a story about someone else, ask yourself first 'Is this my story to tell?' Don't reveal personal details about others without their explicit permission.
- Don't share content from this group without permission - photos, videos, or other content shared in the group cannot be used for any other purpose than originally stated.

Great rules are more than just a list of what's not allowed. Experienced admins recommend using rules to tell members what is encouraged in the group, so members know how they can positively engage with the community.

[last updated July 2022]

---

6. As an admin or moderator of a Church Facebook Group, when should you intervene or take action to keep the space safe?

Short answer: It depends on the context and scenario. The action you take will depend if it is of a pastoral nature, handling of negative comments or heated arguments, group members breaking group rules, content that goes against Methodist policy, or if it is a serious safeguarding concern that needs reporting. In short, you would deal with these issues just as you would in an in-person situation, although some of the methods will be different.

Longer explanation and other scenarios: One of the main differences in an online context is that we often don't own the 'space'. At an on-site church event it's clear when an issue is in a church building, or on church property, or not. Or if it's during a church organised event when we are responsible, or happening at another time. Whereas online, it's harder to define if actions, comments, private messages, or other behavour

are within our jurisdiction. This is why knowing when to intervene, just like in person, depends on the context and is a matter of judgement. But in many cases issues can be handled in a pastoral way: drawing attention to group rules, or social media policy, to gently encourage keeping content appropriate or gracious responses in comments, posts, and messages. It may need a public or private message to gently remind someone or everyone of our safeguarding responsibilities (e.g. if a photo of a child, or confidential information has been shared without permission). Wording can be taken from our Safeguarding Policy about what is acceptable and our stance on racist, sexist, or homophobic content, or any other conduct that would be considered unacceptable in a Christian environment.

However, in some cases, there becomes a distinction here between if the issue is from a church member (e.g. if it's an extension of an in-person safeguarding issue) or if it's a general member of the public (e.g. making inappropriate comments). Where it is the former, it may be appropriate to record evidence (such as taking a screenshot - as digital activity can be deleted) and consult with your minister and/or safeguarding officer. The same processes as would apply in a church building should also be implemented online where there is a major safeguarding concern.

Signposted Resources:

Church of England Social Media Community Guidlines

How to respond to trolls, haters, and honest feedback on Facebook

3 Ways to Handle Negative Feedback on Your Church's Social Pages

[last updated Jan 2022]

Consent Forms

This section applies to obtaining and managing consent of children and adults appearing in church videos, photos, audio or live streams. Where "Church" is used, this should also be taken to mean any circuit, district, youth group, or other official Methodist videos, photos, audio or live stream that is posted online, whether local, regional, or national in nature.

---

1. **What is best practice when it comes to recording video, photos, audio or live streams to be used by the church?**

Short answer: the below questions deal with how and when to obtain formal consent, however, it can often be easier and safer to avoid the need for them altogether. This can be achieved either by not taking photos or videos of any adults or children (not ideal or recommended) or by being creative in how you capture photos and videos.

Longer explanation and other scenarios: when capturing photos or recording video of adults or children without consent, we want to avoid them being 'identifiable' which usually refers to avoiding including people's faces. Here are some creative tips for taking photos and video that keep people safe and bypass the need for formal consent forms to be filled in by not including people's faces:

- Close ups of activities (only including hands, arms, feet, or legs etc.)
- Back of room shots (only showing the backs of heads)
- Shallow focus shots (leaving most of the photo blurred so no faces are visible)
- With a photo that does include faces, use editing software (such as the free online tool Canva) to blur faces, or the whole photo and add text over the top to create a graphic that can be shared

[last updated Nov 2021]

---

2. **What consent and consent forms are needed to include identifiable under 18s in church videos, photos, audio, or live streams that will be used online?**

Short answer: Sometimes it can be best to avoid taking photos or videos of under 18s entirely in a church setting, however, where there is a need, either use the above creative suggestions for avoiding faces, or you must obtain prior written consent and we recommend using the below forms.

Longer explanation and other scenarios: Permission from the parent/guardian of any under 18 needs to be obtained before you can post pictures, videos, audio, or include them in a livestream. If the child is over 12 they are also required to sign the consent form. If the young person is 16 or above and living independently/is estranged from their parents then the form must be signed by the young person and a social worker/youth work/appropriate adult. These will need to be filled out annually. It is worth mentioning that these consent forms only cover activities and images/videos taken within a church capacity. Images of Church activities involving children and young people should not be on personal accounts, unless the children or young people are a part of your family. Images taken outside of this context that are shared on personal accounts are not covered by these guidelines.

Resources:

Links to existing Methodist youth group consent forms (created 2019)

- **For subjects under the age of 12 here**
- **For subjects aged 12-18 years old here**

[last updated Nov 2021]

---

3. **What consent and consent forms are needed for identifiable adults to appear in church videos, photos, audio, live streams that will be used online?**

Short answer: As a minimum you must obtain verbal consent for identifiable adults and provide the ability to opt-out. However, we would still recommend as best practice you should ideally obtain written consent in the same way you would with under 18s.

Longer explanation and other scenarios: If only verbal consent is obtained, then it's important you are clear about what the video/photo/audio/live stream will be used for and where it will be published and distributed. Content cannot be used for any other purpose other than what has been agreed, which is why using a consent form is best practice. For more details on best practice when live streaming a service or event, see question 1 under the Live Streaming and Online Worship section.

Resources:
Yorkshire North & East District
Example consent form for adults (created 2022)

[last updated Nov 2021]

---

4. **Does consent also need to be sought for videos people have filmed themselves from home and sent in for the church to use in online worship?**

Short answer: No written or verbal consent is needed - as videos are being provided by the individual then consent is implied. However, the content cannot be used for any other purpose other than what has been agreed. It's good practice to keep emails (or other written communication, if applicable) as a record of consent, in lieu of a consent form.

Longer explanation and other scenarios: In many cases, verbal or written consent will have been obtained anyway as part of arranging videos to be filmed at home for online worship (such as confirming with someone on the phone that they are happy to record a reading, or arranging it via email). Records of email correspondence can then be kept as proof of written consent, but either way participants have the option to opt-in when they provide the video, or not as they wish. However, it is important to make clear what purpose the video/photo/audio is to be used for and where it will be published or distributed.

[last updated Nov 2021]

---

5. **Should churches or admins share posts on social media from other accounts that contain photos/videos of under 18s? How do we know if consent has been obtained correctly?**

Short answer: Photos/videos can be shared if it is posted by a trusted organisation, or if a parent has tagged your church in the post. Otherwise we would advise against sharing any photos/videos of under 18s on social media that you haven't obtained consent for yourself.

Longer explanation and other scenarios: Parents sharing photos of their own children on social media, and tagging the church in the post, are ok to share on the church account (if that is a feature of the platform, such as Facebook and Twitter. On Instagram you can share to Stories, but you shouldn't repost the photo/video on your feed. YouTube doesn't have a feature for sharing in that way) - consent has been given here by the tagging feature, however, it is still best practice to comment on the post or message to ask if it would be ok to share. The photos/videos must not be used in any other way. You must not download the photos/videos, or post them on your church website. If you wish to do this, written permission must be sought. If a parent hasn't tagged the church in the post, but the photos/videos are still publicly available, then we'd recommend avoiding sharing the content, as we don't know the context or safeguarding situation. We would generally discourage the sharing of content to a church account that includes photos/videos of under 18s, unless it is clear that parental permission has been given or it is part of publicity used by a trusted organisation who will have been responsible for obtaining consent.

[last updated Nov 2021]

---

6. **Should photos/videos of identifiable under 18s posted online in the past without correct permissions, sometimes having been online for many years already, be removed?**

Short answer: Yes, we would encourage this as best practice, and as such conduct some form of regular audit of online channels to check correct permissions are in place. It's important to keep records of photo/video consent forms for identifiable under 18s.

Longer explanation and other scenarios: Whilst it does entail quite a bit of work and regular upkeep, we would encourage revisiting your church social media accounts and websites as best practice. It's not a required task, but we would encourage a regular (although we haven't defined what time frame 'regular' means in your context) audit of church social media channels and assets to check if proper consent was given - particularly for photos/videos containing identifiable under 18s. It's important to keep records of this. If a church believes that consent was obtained for an under 18, but there isn't a written record of it, then the photo/video should be removed.

[last updated Nov 2021]

---

7. **Do you need verbal or written permission to record a Zoom meeting to publish online? Does this change if there are under 18s present?**

See answer in "Zoom & video conferencing" section

---

8. **Should all church staff, leadership and volunteers have and use separate professional devices for use in online worship, photography, live streaming, running software, zoom, storing content?**

See answer in "Live Streaming and Online Worship" section

Live Streaming & Online Worship

This section applies to live streaming of church services or other events, pre-recorded or live online worship, or any hybrid model that contains elements of either. Where the term "church" is used, this should also be taken to mean any circuit, district, youth group, or other official Methodist live stream or online worship, whether local, regional, or national in nature.

General advice on live streaming and online worship for churches:
District Digital Resources Hub (Yorkshire North and East Methodist District)

---

1. **Live streaming permission and consent - best practice for live streaming a church service**

Short answer: The same guidance applies for live streaming as for photos and videos (**see questions 1, 2 and 3 of the Consent Form section**). In summary, you need consent from anyone who is visibly or audibly identifiable in your live stream, just as you would for video or photos. Publicise in advance when and where livestreaming will happen so people can "opt-out". Have signs up on the day informing people that livestreaming is happening (resources below). Create a space where you can "opt-out" of being seen / recorded on the live stream (resources below). It's good practice to ask all the musicians, singers, speakers etc. for their consent before broadcasting their 'performance'. Carefully consider what is in view of the camera, i.e. check that the background is professional and does not contain images, information, or people that should not be shared. Be mindful of the need for confidentiality; especially if live-streaming from a church where other adults or children are present. Even if they are not visible on camera, will their voices be picked up by the microphones? If applicable, make sure to moderate and keep an eye on comments and activity on your live stream. Familiarise yourself with social media or Zoom settings (whatever platform you are using to live stream) that can be used to help moderate and manage your live stream.

Longer explanation and other scenarios:

The same guidance for photos and videos applies to live streaming, and so it's worth familiarising yourself with the Consent Forms chapter of this document first. However, live streaming an event or church service presents additional challanges and application of safeguarding policy.

What if children wander into the live stream area? We would suggest that as long as you make it really clear where the live streaming area is, and what is visible on/off camera, then it would be the responsibility of parents (particularly those who haven't been before) to ensure children don't wander into this area. But this needs to be made clear to them. It would be good practice to allow a good amount space for children to wander about off camera. It can be tricky live streaming with children wandering about in

church, but we'd suggest that you only need to seek written permission and fill in consent forms for children who are intentionally going to participate in a service. Try to keep it so that children don't appear on the live stream, and seek written permission when you intentionally want someone to be involved / appear. To achieve this, it might be a good idea to include live streaming as part of your 12 monthly consent forms for junior church, which will let you know if there are children that definitely shouldn't be appearing on the stream.

How do we protect against the unlikely situation of a child doing something inappropriate during a live stream? (such as toddlers or junior church) There isn't much you can do to mitigate against this in advance, particularly with younger children. Again we would suggest that it would be the parents responsibility to keep children wandering into the live stream area. But you need a process in place for if this, or something else inappropriate, were to happen, so best practice would be to make sure your technically team / person has the ability and process in place to be able to cut the stream, change cameras, or switch to a holding screen in the event of an issue, and the feed can then be resumed after the situation is resolved.

What if we want to invite children up front to engage with a children's address or all-age activity? To avoid the need for every child to have a written constent form, or having to not let certain children be involved, it's a good idea to have an area at the front where you can invite children up, but where they won't appear on the camera (ideally without making it obvious to those in the church). I.e. switching to a close up camera would allow for children and young people to come forward and interact, whilst the live stream only shows a view of the person leading the service.

Can a conset form cover all live streaming in the church? It depends how your consent form is worded, as it needs to be specific. So it's unlikely to be good practice to have it broad enough to cover all church live streams – but it could cover all Sunday morning live streams. Communication is important, and parents must have the ability to withdraw their consent at any time under GDPR. Even if you already have permission through the 12 monthly forms, it's still best practice to remind and check with parents on the day.

Is verbal permission enough for instances where it's not possible to get immediate written permission, for instance if a family is late to the service or a newcomer? Written permission is needed, particularly for under 18s, however it's always better to have verbal permission than no permission. If appearing in the live stream is a likely event for newcomers, then maybe have some simple consent forms on hand in the church for parents to sign on arrival – this is often done really well at conferences etc. (however obviously this isn't ideal, and probably not a great first impression, so if it can be avoided we would encourage it – but it might be a good backup if needed).

Do we need written permission for children to be on live stream when they are children of those employed by church, minsiter, or volunteer? All the same policy, guidance and consent will apply to children of church staff as it would to any other children and young

people. The parents who are church staff might be happy, but it's as much about the church having a paper trail as anything else.

How do we enable children to feel welcome in the space when we have no-go areas because of the live stream? Especially for those children who like to run around, or want to be up front in the live stream area? When it comes to long term solutions for allowing flexibility for children, we would suggest investing in equipment and human resources that allow you to move/zoom cameras during the service. As such you should be able to change what's visible in the frame to avoid showing children (of course making sure you're not showing anything in the camera-free zones marked out in the church). This would potentially allow children to move more freely (within some constraints) whilst ensuring the don't appear on the live stream.

Resources:
Live Streaming guidance including safeguarding (Church of Scotland)

[last updated July 22]

---

2. **What is safeguarding best practice when it comes to moderating live streams and comments on live streams? When should you intervene or take action to keep the space safe?**

See question 6 under the Church Facebook Groups section

---

3. **Can under 18s comment and interact with adults on a church live stream?**

Short answer: Under 18s can comment and interact on a church live stream, as long as there is sufficient moderation in place. It is not possible to prohibit under 18s from interacting, as you are unlikely to know on social media the ages of those commenting, unless you know them personally. An official church account, and those in leadership roles, should take every effort not to follow anyone under 18, or like or comment on any posts they make. However, it is ok for a church account, or adults in leadership roles, to respond to comments or interact in an appropriate way in a public space with an under 18 such as within the comments of a church live stream.

Longer explanation and other scenarios: We would not encourage Church accounts, or those in leadership roles, to follow or friend under 18s, however, if there is to be engagement with young people on social media, the best way would be public engagement via your church account (such as responding to public comments). Church accounts can respond to comments on their own posts or live streams from under 18s, as in many cases the age of the commenter won't be obvious or even accessible.

Under 18s are also able to interact with other adults (not in leadership roles - i.e. the general congregation) within the comments or chat of a live stream as long as there is

sufficient moderation. See **questions 3, 5 and 6** of the Church Facebook Groups section for guidance on moderation of an online space.

If you are contacted directly on a church social media account by a known under 18, alert the other admin or account holder that this has happened in order to remain accountable. Do not engage in conversation beyond responding to simple queries.

[last updated July 22]

---

4. **Should all church staff, leadership and volunteers have and use separate professional devices for use in online worship, photography, live streaming, running software, zoom, storing content?**

Short answer: Ideally, yes. We should be using church owned equipment, particularly where we are storing data or capturing images/videos of under 18s. Software and online accounts should be owned by the church, but there is more flexibility here where no data or images/videos are captured. The same would be true for using personal equipment to live stream, where no data is recorded.

Longer explanation and other scenarios:

In practice this can become costly and can be difficult to achieve, especially when members of our congregation or staff have personal devices that they are willing to lend for the work of the church. We should try to follow best practice where we can, but where personal devices are used, ensure security measures are in place for protecting sensitive data (using secure devices, having passcodes on phones and computers, storing technology, memory cards, and data sticks in a locked safe, and deleting any photos, videos or data once they are no longer needed). Only those who have been safer recruited to a formal role in the church (see question 1 in the Church Social Media Accounts section) should be using personal or church devices to run online worship, live streams, or capturing and storing church photos/videos/data of any form. We should be using church owned Zoom accounts for public online worship, whether free or paid, and not someone's personal account (an exception may be if the Zoom account is owned by your minister, or you're attending a private church meeting)

[last updated August 22]

---

5. **Do you need verbal or written permission to record a Zoom meeting to publish online? Does this change if there are under 18s present?**

See answer in "Zoom & video conferencing" section

---

6. **Can those on Safeguarding Contracts interact with a church live stream or join Zoom online worship? Can they join an online church in a different geographical area?**

Short answer: If their contract allows them to be online, and there's no other circumstances that would prevent them joining, then engaging with online worship in any form is acceptable as long as all other digital safeguarding guidance in this document is followed (see below for more details on this). When joining online worship from a different church or geographic area, then the same process should be followed as attending a physical building, and permission should be sort from their monitoring group to attend a different church's online worship.

Longer explanation and other scenarios: When best practice is applied online with safeguarding (such as disabling private chat in Zoom, or having safer recruited and trained social media admins and moderators) then the risk relating to those on Safeguarding Contracts is potentially very low. There is little-to-no opportunity for an individual to engage with anyone else privately or one-to–one, and any contact made will be able to be monitored by those leading online worship or those moderating it via technology. Whilst it is best practice for those on safeguarding contracts to seek permission from their monitoring group to attend a different church's online worship, this is hard (sometimes impossible) to actually monitor and track. It relies on the individual to be honest and work on a trust based system. This is a key reason why it's really important for all churches to follow digital safeguarding best practice as laid out across this whole document - you might never know when an at-risk individual, or someone who poses a potencial risk, might be engaging with your church online or attending your online worhsip.

Zoom & Video Conferencing

This section applies to churches specifically using the video conferencing platform "Zoom" for meetings, online worship, or other events, however much of the advice will also be applicable to other programs (such as Microsoft Teams, Google Meet, or the video calling feature on a WhatsApp or Facebook Messenger group chat). Where the term "church" is used, this should also be taken to mean any circuit, district, youth group, or other official Methodist meeting conducted on Zoom, whether local, regional, or national in nature.

General advice on using Zoom for churches:
District Digital Resources Hub (Yorkshire North and East Methodist District)

---

1. **How to distinguish between a church-run Zoom meeting and a meeting set up in a personal capacity by a sub-group or group of friends in the church?**

Short answer: It depends who has the Zoom account and is "host" of the meeting

Longer explanation and other scenarios: If the Zoom "host" (person who has set up the zoom meeting and is normally leading the session) has a role in the church (minister, lay employee, volunteer, or anyone in a position of leadership) and the group contains other church affiliated people, then it is a church-run Zoom meeting and must follow Methodist Church safeguarding practice (i.e. the guidance in this section). If the Zoom meeting has been set up by someone outside the church, or anyone in the church who doesn't hold a role (as described above) in order to keep in touch with friends in the church (for example a mum's group set up by someone who attends messy church, or young persons group set up by one of the young people themselves, or an online housegroup/small group set up with friends who go to church but it hasn't been organised 'officially') - then this can be considered a personal / 'unofficial' group and not the responsibility of the church. The safeguarding practice would be down to the individuals in the group, and whilst we would encourage best practice, the church is not responsible for ensuring this is followed.

[last updated Feb 2022]

---

2. **Should password holders of church Zoom accounts and/or 'hosts' of Zoom meetings have a DBS check, and/or have undertaken the Methodist safeguarding training?**

Short answer: Zoom accounts held by youth groups, or those 'hosting' or leading Zoom meetings aimed at children (under 18s) must have a children's worker (unregulated) DBS check and undertaken the Methodist Safeguarding Training.

However, those with access to church-run Zoom accounts or those who regularly host / lead Zoom meetings not predominantly aimed at under 18s don't need a DBS but should have been safer recruited - this is likely already in place as part of a wider or different role, such as minister, worship leader, lay employee, or steward etc. (see question 1 in the Church Social Media Accounts section for more details).

Longer explanation and other scenarios: It can be tricky to identify who the 'host' is, as this can be transferred during a Zoom meeting and the password holder of the 'host' account (who set up the meeting) doesn't always have to be present for the meeting to take place. This may also be different from the person "leading" the meeting or session. And as mentioned in question 1, there can be some blurred lines in where a Zoom meeting is personal or comes under the banner of the church. Where the Zoom meeting is predominately for or aimed at adults, the distinction between these roles is less important, but where it is a church-run Zoom meeting (see question 1) we would suggest that meetings should have at least one 'host' who holds a church role (minister, lay employee, or volunteer) and has been safer recruited.

Whilst there is no need to undertake Methodist Safeguarding Training we would suggest that all zoom hosts familiarise themselves with the content in this section so they are able to deal with issues that may arise and are aware of safeguarding best practice in Zoom. You can also read the below questions for more details on using Zoom with under 18s, but do also refer to the Youth Groups, Children & Young People section.

The above guidance assumes a distinction between Zoom meetings that contain under 18s and those for adults. See question 4 below for details on holding Zoom meetings that contain a mix of adults and under 18s

[last updated Feb 2022]

---

3. What is best practice for using the chat function in Zoom?

Short answer: Private chat should always be turned off in Zoom, particularly if there are any under 18s present. However, public chat is fine to have enabled as long as it is monitored.

Longer explanation and other scenarios: The private chat feature allows participants to send private messages to other participants while in a meeting, this can post a safeguarding concern, particularly with under 18s present in the meeting, as private messages between participants are not viewable by the host. Disabling private chat prevents participants from privately messaging other participants, but still allows participants and the host to send private messages to each other. Hosts can also disable chat for everyone in the meeting, however, this isn't required from a safeguarding perspective as long as the host, or co-hosts, are able to monitor comments. For more on how to monitor the chat, and when to take action, see **questions 3, 5 and 6** of the Church

Facebook Groups section for guidance on moderation of an online space. See question 5 below for specific settings that Zoom hosts and co–hosts should be aware of how to use.

[last updated Aug 2022]

---

4. **What are the best practices for hosting a Zoom youth group or meeting for all under 18 year olds?**

See answer under the Youth Groups, Children & Young People section

---

5. **Can you have a Zoom meeting that contains a mix of under 18s and adults?**

Short answer: Zoom Groups specifically for Youth Groups or under 18s should not contain adults who aren't youth group leaders or safer recruited. However, Church or general Zoom meetings (such as online worship) could, in principal, contain a mix of under 18s and adults as long as the Zoome meeting has good guidelines, rules, and moderating. The WhatsApp section details how Adults can communicate with under 18s within a group (although not ideal) where certain safeguarding measures are in place, and this is the same principle that applies to a Zoom meeting. In this context all communication between the under and over 18 year olds is being monitored. Do follow all the Zoom best practice in this setion, and take a detailed look at question 7 on running a Zoom for young people in the Youth Groups, Children & Young People section

Longer explanation and other scenarios: See more guidance for Facebook Groups specifically for under 18s under the Youth Groups, Children & Young People section.

It's important to note that Zoom's advice around under 16s using the platform is:
"Children under 16 cannot create a Zoom account. A parent or guardian may, however, permit the child to use that parent or guardian's account with their supervision."

Ensure there are at least two leaders, who have been recruited using the Safer Recruitment processes (references and DBS checks) in each virtual meeting (and make sure the leaders 'arrive' before the group does). You will need parental consent to include their child in any virtual meeting space and, for those under 16, the parents/carers will need to be the Zoom account holders and the link for the meeting should be sent to them. We also recommend that parents/guardians are asked to supervise the Zoom call. Do not record the meeting. In the settings for your Zoom meeting you should disable the one-to-one anonymous chat function so that participants cannot send private messages that are not seen by the wider group. You may also want to consider disabling screen share and only allowing this if needed for a particular activity.

Hosts and Co-hosts also have access to mutile safety features. Make sure to have a password set, the 'waiting room' enabled, the option so people can't rejoin the meeting if they are removed by a host, disable screensharing, and 'mute on entry' selected. Have

virtual 'stewards' (co-hosts) who can monitor and keep an eye on everything, including muting people who interrupt or as a final measure, removing people from the meeting. If you are particularly worried about Zoom bombing, or don't have anyone with the technical ability to administer the above, then there is more thorough guidance from the Methodist Church here. We would encourage all group admins and moderators to familiarise themselves with these practical safety features.

[last updated Aug 2022]

---

6. Should you share Church Zoom links online?

There is some debate on whether it's safe to share Zoom details and service links on social media publicly due to their being an initial spate of 'zoom booming' during the early part of the pandemic. However, as long as you have security features enabled and in place, you are perfectly safe to share details online. Make sure to have a password set, the 'waiting room' enabled, the option so people can't rejoin the meeting if they are removed by a host, disable screensharing, and 'mute on entry' selected. Have virtual 'stewards' (co-hosts) who can monitor and keep an eye on everything, including muting people who interrupt or as a final measure, removing people from the meeting. If you are particularly worried about Zoom bombing, or don't have anyone with the technical ability to administer the above, then there is more thorough guidance from the Methodist Church here

[last updated Aug 2022]

---

7. Do you need verbal or written permission to record a Zoom meeting to publish online? Does this change if there are under 18s present?

Short answer: The same guidance applies for recording or sharing a Zoom meeting as for photos and videos (**see questions 1, 2 and 3 of the Consent Form section**). In summary, you need consent from anyone who is visibly or audibly identifiable in your zoom screenshot or recording, just as you would for video or photos. As a minimum you must obtain verbal consent for identifiable adults and provide the ability to opt-out. However, we would still recommend as best practice you should ideally obtain written consent in the same way you would with under 18s, so that you have a paper trail. Under 18s specific Zoom meetings, such as an online youth group, should not be recorded.

Longer explanation and other scenarios:

For under 18s in a mixed Zoom event, permission from the parent/guardian needs to be obtained before you can post screenshots or record a Zoom meeting. If the child is over 12 they are also required to sign the consent form. If the young person is 16 or above and

living independently/is estranged from their parents then the form must be signed by the young person and a social worker/youth work/appropriate adult.

For adults, if only verbal consent is obtained, then it's important you are clear about what the recording will be used for and where it will be published and distributed. Content cannot be used for any other purpose other than what has been agreed, which is why using a consent form is best practice. For more details on best practice when live streaming a Zoom meeting, see question 1 under the Live Streaming and Online Worship section.

[last updated Aug 2022]

---

8. Best practice guidance for those attending a zoom meeting

Short answer: Just like with Facebook Groups or WhatsApp groups, Zoom is an interactive online space that requires a commitment by participants to abide by agreed apon rules, just as much as it is down to leaders and hosts to follow safeguarding process and moderate the space. As with any other form of online socialising, the behaviour of the users play a big part in how safe Zoom is. Cyberbullying, giving away personal information, inappropriate images or messages and peer pressure are universal issues that can pose a risk on any service.

Example Zoom 'rules' / agreement for those joining

- Use your real name (you can change this by clicking "rename")
- Check your background is appropriate or you are using an appropriate virtual background image
- Mute yourself when others are speaking
- Use the 'raise hand' feature in Zoom to indicate you would like to contribute
- All comments and opinions expressed within the Zoom group are solely the author's and may not reflect the opinions and beliefs of the Methodist Church or its affiliated groups.
- Remember to be considerate, respectful, and inclusive to all within the group.
- Please refrain from commenting or sharing content (including videos or links in the chat) that could be interpretated as inappropriate, demeaning, or inflammatory.
- Maintain confidentiality - If telling a story about someone else, ask yourself first 'Is this my story to tell?' Don't reveal personal details about others without their explicit permission.
- Please pass any concerns regarding the group or its members to the Zoom host or co-host. Any safeguarding concerns should be reported to the minister or church safeguarding officer.

[last updated Aug 2022]

WhatsApp

This section applies to churches using the application WhatsApp, particularly the group chat function. For information on personal, or private one-to-one, use of WhatsApp see information in the "Email, Texting, & other 1-1 communication" section. Where the term "church" is used, this should also be taken to mean any circuit, district, youth group, or other official Methodist organisation using WhatsApp, whether local, regional, or national in nature.

---

1. **How to distinguish between a church-run WhatsApp group chat and a chat set up in a personal capacity by a sub-group or group of friends in the church?**

Short answer: It depends who is the "admin" of the WhatsApp group

Longer explanation and other scenarios: If the group "Admin" (person who has set up the group chat) has a role in the church (minister, lay employee, volunteer, or anyone in a position of leadership) and the group contains other church affiliated people, then it is a church-run group chat and must follow Methodist Church safeguarding practice (i.e. the guidance in this section). If the group chat has been set up by someone outside the church, or anyone in the church who doesn't hold a role (as described above) in order to keep in touch with friends in the church (for example a mum's group set up by someone who attends messy church, or young persons group set up by one of the young people themselves, or prayer chain set up with a group of friends who go to church but it hasn't been organised 'officially') - then this can be considered a personal / 'unofficial' group and not the responsibility of the church. The safeguarding practice would be down to the individuals in the group, and whilst we would encourage best practice, the church is not responsible for ensuring this is followed.

[last updated Jan 2022]

---

2. **Should WhatApp Group admins have a DBS check, and/or have undertaken the Methodist safeguarding training? And have the same safer recruitment process as church social media account admins?**

Short answer: for any official church / circuit / district run WhatsApp Group (or any WhatsApp Group set up or run by a Methodist organisation) all the same guidance applies as was provided for church social media account admins (see question 1 from the church social media accounts section). However, if you're already recruited to an online role, such as admin of a church Facebook Page, then the Social Media Access form and other safer recruitment processes only need to be done once.

Longer explanation and other scenarios: Admins of WhatsApp Groups aimed at children (under 18s) must have a children's worker (unregulated) DBS check. However, those with access to church-run WhatsApp Groups (not predominantly aimed at under 18s), whether employed or volunteers, don't need a DBS but should have been safer recruited: (a single all-in-one form is provided below that covers *'digital key holder form', 'role description', 'self-declaration SD/4' and 'code of conduct'*). It is not a requirement for group admins to do the Methodist Safeguarding Training (Foundation or Advanced) however we would suggest that all WhatsApp Group admins undertake specific training in the form of reading our 'code of practice'. Safer recruitment to social media roles only needs to be done once, as it's common for employees and volunteers to be admins of multiple accounts, platforms, and for different churches. There is space on the Church Social Media Access form to list multiple social media accounts so the form only needs to be completed once.

For more details and resources, see answer to question 1 in the 'Church Social Media Accounts' section

[last updated Jan 2022]

---

3. What is best practice for adding people to a church WhatsApp group chat?

Short answer: As a minimum you need to have consent from people before adding them to a WhatsApp group chat, as all the other members will be able to see and access their phone number. However, we would also recommended using our WhatsApp form below as the best practice for adding people. This is a short agreement and guidelines that people can agree to before they are added to the group, making expectations and boundaries clear.

Longer explanation and other scenarios: This group agreement/guidelines has been developed to encourage healthy boundaries on WhatsApp to ensure that people find WhatsApp groups safe spaces to communicate with others.

Resources
WhatsApp Group Agreement

[last updated Feb 2022]

---

4. What group rules or code of conduct should you have in a church WhatsApp group?

Short answer: The below suggested guidelines and code of conduct have been taken from our WhatsApp group agreement form, which we would recommend using for all members joining your chat.

- You cannot anonymise yourself when joining a WhatsApp group; your number will be visible by other members. Please do not pass on the contact details of any group member to others without their consent.
- All comments and opinions expressed within the WhatsApp group are solely the author's and may not reflect the opinions and beliefs of the Methodist Church or its affiliated groups.
- Please do not contact people in the group privately (outside the WhatsApp group) unless you have first asked their permission to do so.
- Remember to be considerate, respectful, and inclusive to all within the group.
- Please refrain from commenting or sharing content (including videos or pictures) that could be interpretated as inappropriate, demeaning, or inflammatory.
- Consider all messages before you send them. Are they appropriate? Are you sending it to the right group?
- Be mindful of sharing any personal information, including information about others. Always obtain consent when sharing information if it relates to other people e.g., when asking for prayer for a friend or family member.

- Please pass any concerns regarding the group or its members to the WhatsApp group administrator. Any safeguarding concerns should be reported to the minister or church safeguarding officer.
- Keep topics of conversation to the intended purpose of the WhatsApp group.
- Please don't be offended if people leave the group, many people are busy and struggle to keep up with the demands of responding to messages. Do not feel pressurised into staying with the group, you can leave at any point.
- Try to keep interactions to a reasonable time e.g., no messages before 8am or after 10pm unless it is an emergency.
- Group administrators will always ask an individual before adding them to the group. If you would like a person adding to the group, please seek consent to pass their details to the group administrator.

As well as the above, for groups with under 18s, the following should be considered:

- Consent should be obtained from a parent or guardian for a young person to join a WhatsApp group.
- Groups for young people should be monitored by two adult group leaders who are safely recruited to the role and have appropriate DBS checks and safeguarding training.
- Group leaders should not contact young people on WhatsApp outside of the group chat.
- Group leaders should ideally use a church issued phone where this is possible.
- Other adults, including parents, should not be added to the WhatsApp group unless they are safely recruited to work with children and young people on behalf of the Methodist Church, with appropriate DBS checks and training.

Resources
WhatsApp Group Agreement

[last updated Feb 2022]

---

5. Can a church WhatsApp group contain a mix of under 18s and adults?

Short answer: Whilst this is not best practice in many contexts, as long as good safeguarding guidance is followed, it can be ok in certain situations to have a mixed group, where all communication is actively monitored. Where church WhatsApp groups have a mix of adults and under 18s, it is even more important that all members agree to the code of conduct and this is presented to them before they join. However, where possible we would advise against having a mixed group, due to the nature of WhatsApp providing all group members access to the under 18s personal phone number. For more on how to monitor the chat, and when to take action, see **questions 3, 5 and 6** of the Church Facebook Groups section for guidance on moderation of an online space.

Please read and implement the best practive guidance in questions 1, 2, and 3 above to ensure your church WhatsApp group is a safe space for both adults and under 18s.

[last updated Aug 2022]

---

6. **As an admin or moderator of a Church WhatsApp Group, when should you intervene or take action to keep the space safe?**

Short answer: see **questions 3, 5 and 6** of the Church Facebook Groups section for guidance on moderation of an online space. As with any other form of online socialising, the behaviour of the users play a big part in how safe WhatsApp is. Cyberbullying, giving away personal information, inappropriate images or messages and peer pressure are universal issues that can pose a risk on any service.

Longer explanation and other scenarios: There are two ways by which you can become the admin of a WhatsApp group; 1) creating the group — automatically makes you an Admin 2) being appointed as an admin (refer to question 1 above). By default, any group participants can send messages and change group information including, the group subject, icon, or description. However, a group admin can change group settings to allow only admins to edit group info or send messages. Group admins can also add members, delete members, edit group info, or delete the group. As a WhatsApp group admin, do familise yourself with the current WhatsApp settings and features so you are effectively able to moderate the space in a safe way.

[last updated Aug 2022]

Church Websites

This section applies to church websites. Where the term "church websites" is used, this should also be taken to mean any circuit, district, youth group, or other official Methodist website, whether local, regional, or national in nature.

General advice on websites for churches:
District Digital Resources Hub (Yorkshire North and East Methodist District)

---

1. **Should editors of Church Websites have a DBS check, and/or have undertaken the Methodist safeguarding training? And have the same safer recruitment process as church social media admins?**

Short answer: for any official church / circuit / district run website (or any website set up or run by a Methodist organisation) all the same guidance applies as was provided for church social media admins (see question 1 from the church social media accounts

section). However, if you're already recruited to an online role, such as admin of a church Facebook Page, then the Social Media Access form and other safer recruitment processes only need to be done once.

Longer explanation and other scenarios: Editors of church websites aimed at children (under 18s) should have a children's worker (unregulated) DBS check. However, those with access to church-run websites (not predominantly aimed at under 18s), whether employed or volunteers, don't need a DBS but should have been safer recruited: (a single all-in-one form is provided below that covers *'digital key holder form', 'role description', 'self-declaration SD/4' and 'code of conduct'*). It is not a requirement for editors of church websites to do the Methodist Safeguarding Training (Foundation or Advanced) however we would suggest that all editors of church websites undertake specific training in the form of reading parts of this guidance document. Safer recruitment to social media roles only needs to be done once, as it's common for employees and volunteers to be admins of multiple accounts, platforms, and for different churches. There is space on the Church Social Media Access form to list multiple websites, alongside social media accounts, so the form only needs to be completed once.

For more details, see answer to question 1 in the 'Church Social Media Accounts' section

Resources:

- **Church Social Media Access Form**
  (all-in-one 'digital key holder form', 'role description', 'self-declaration' and 'code of conduct' to be signed by those with access to church social media accounts)

- Code of Conduct (extract from above document)

---

2. Should photos/videos of identifiable under 18s posted online in the past without correct permissions, sometimes having been online for many years already, be removed?

Short answer: Yes, we would encourage this as best practice, and as such conduct some form of regular audit of online channels to check correct permissions are in place. It's important to keep records of photo/video consent forms for identifiable under 18s.

Longer explanation and other scenarios: Whilst it does entail quite a bit of work and regular upkeep, we would encourage revisiting your church website as best practice. It's not a required task, but we would encourage a regular (although we haven't defined what time frame 'regular' means in your context) audit of your church website and assets to check if proper consent was given - particularly for photos/videos containing identifiable under 18s. It's important to keep records of this. If a church believes that consent was obtained for an under 18, but there isn't a written record of it, then the photo/video should be removed.

[last updated Nov 2021]

---

3. Best practices for accessing websites through church public Wi-Fi

Many churches povide public WiFi and it should be considered is any safeguarding measures need to be put in place for those accessing websites through the church WiFi. For exmaple, filtering and monitoring could be employed to block harmful content or prevent access to certain websites whist on the church network.

The acceptable use policy should be displayed, or be accessible to users by means of a prominent hyperlink, before the user gains access to the Wi-Fi network.

Resources
Guest Wi-Fi Acceptable Use Policy (from the Connexion)
Guide for internet filtering and monitoring (UK Safer Internet Centre) - for education settings, but useful info for churches

[last updated Aug 2022]

Individual Social Media Use

This section applies to Methodists using Social Media in a personal capacity, but particularly refers to church / circuit / district employees, volunteers, ministers, and those in leadership positions.

General advice on how to set up social media accounts as an individual:
How to get started with Facebook (Methodist pdf)
Setting up an Instagram account (Church of England blog)

Online Safety advice for individuals, parents, or children:
See question 15 under the Youth Groups, Children & Young People section

---

1. **Should you create a seperate 'work' social media account as a minister, lay employee, or volunteer?**

Short answer: This is fine to do on Twitter and Instagram, however, it is against Facebook's community standards and so you should only ever have one Facebook account.

Longer explanation and other scenarios:

Facebook is a community where people use their authentic identities. It's against the Facebook Community Standards to maintain more than one personal account. Facebook do NOT allow misrepresenting your identity by:

- Using a name that is not the authentic name you go by in everyday life
- Providing a false date of birth.
- Creating a single account that represents or is used by more than one person.
- Maintaining multiple accounts as a single user.

If you're a public figure, such as a minister, you can have "followers" as well as friends, who only see your public posts, thus enabling you to create a distinction between work and personal life. Find out more about followers on Facebook here

If you need to use your personal Facebook account for work purposes, we would suggest familiarising yourself with Facebook privacy settings, enabling you to restrict what others see on your profile.

[last updated Aug 2022]

---

2. **What is best practice guidance for using social media in a personal capacity as an employee, minister, volunteer, or in a leadership position?**

It is your responsibility to be aware of and to follow Methodist Safeguarding Policy and the digital safeguarding guidance set out in this document.

General

If you comment on any aspect of the work of the organisation or any policy issue for the organisation, you must clearly identify yourself as a paid employee, or volunteer in a leadership position, of the organisation in your postings, and respond in line with the views of the organisation. If you wish to raise concerns about the work or policies within the organisation, your line manager is the appropriate channel.

By virtue of identifying yourself as an employee, or volunteer in leadership position, of the Methodist Church within a social network, you are nurturing connection with your colleagues and the global Christian community. You must ensure that content associated with you is consistent with your work and the Christian values of love, tolerance and forgiveness.

Interactions with under 18s

Leaders should not add or accept requests to follow or friend young people (under 18) from personal profiles if they are involved with the church or youth group. It is fine to be friends with your own children or Godchildren if they are part of the church or youth group. If you take on a leadership role in the Church, you should not follow / have any friends on your personal social media who are under 18 who are involved in the church. If you currently have friends under 18 you should explain to them that you now have a leadership role and that requires you not to have contact with under 18s via your personal social media accounts. If a young person turns 18 and becomes a leader, they should ideally unfriend any young people under 18 that are involved in their youth group and follow the guidance for group leaders. This is part of forming new boundaries as a leader. If, while on a personal account, you do see posts from young people (e.g. shared by someone you are friends with) do not like, react or comment on the posts. If you work with children and young people in the church, your personal accounts should have all its privacy settings set as high as they can be so that a young person cannot access your photos, posts etc, and you have to approve requests to friend/follow you.

A minister or leader, due to the nature of their role, may have a public profile for personal use. This means that anyone can follow you and/or see your posts, however this is still a personal account and not a church social media account. In order to keep clear boundaries, it should not be treated (or encouraged to be used by the public) as official communication from your church or youth group. It should not be used (or encouraged to be used by young people) as a space to engage with under 18s. This is a grey area, as a minister or leader with a public personal profile might share publicity, posts, and other content from their church as they engage publicly with the wider community, but the public and especially young people should be directed to official church channels to receive this communication directly. Leaders can communicate with under 18s in a public

context, such as in comments of a church post on social media (see more detail in the Church Social Media Accounts section), or within a public church Facebook Group (see detail in the Church Facebook Groups section), however this shouldn't happen on a personal account. So leaders shouldn't respond to comments made on personal public posts.

See question 9 in the Church Social Media Accounts section on social media policy for more details and question 1 for a **code of conduct** for staff and volunteers.

Resources
Methodist Socia Media conduct - general values for all
Example Social Media guidance & policy for ministers & staff (Diocese of Gloucester)
Methodist Social Media Guidlines - interacting with under18s (from 2019)

How to use Facebook privacy settings and tools
How to use Instagram privacy settings and tools

[last updated Nov 2021]

---

3. **Can under 18s who have a role in the church / leadership position be friends with other under 18s, or would they need to unfriend all their peers?**

If you take on a leadership role in the Church, you should not follow / have any friends on your personal social media who are under 18 who are involved in the church. However, those under 18 in leadership positions wouldn't need to unfriend or unfollow other under 18s, as they are not adults. But they would need to follow all other safeguarding practice, as outlined in this document, as part of forming new boundaries as a leader.

[last updated Aug 2022]

---

4. **What should you do if you come across young people in your church under 13 who have social media accounts?**

Short answer: This will often need to be dealt with pastorally by someone in a church leadership role, or your safeguarding officer. You can also report accounts through Facebook and other platforms for being underage and they will investigate.

Longer explanation and other scenarios:
All social media platforms have age restrictions. The reason all social media has age restrictions is usually because in law organisations operating online services are not allowed to collect personal information of anyone under the age of 13 without parental permission. To avoid the necessity of obtaining parental permission for any user under the age of 13, most services have instead chosen to have age restrictions. Others have higher age restrictions due to issues around GDPR and safeguarding.

For clarity, for all of the below, the age restriction means that you cannot use the platform in any way if you are under the age requirement. It doesn't only apply to creating an account on that platform, which is a common misconception (the phrasing in the terms & conditions is usually "to use our services"). For example, on YouTube you have to be 13 to watch any video on the platform (unless viewing on the YouTube Kids app).

- Facebook: 13+
- Twitter: 13+
- Instagram: 13+
- YouTube: 13+
- YouTube Kids: 0+ (if enabled by a parent or legal guardian)
- WhatsApp: 16+
- Zoom: 16+ (note: under 16s cannot create an account or use the platform on their own, however Zoom have clarified that parents can give permission for an under 16 to use their acccount if they are suppervised during the meeting)
- TikTok: 13+
- Snapchat: 13+
- Pinterest: 13+
- LinkedIn: 16+

[last updated Aug 2022]

---

5. **What are the best practices for leaders communicating with under 18s via electronic means?** (Social Media direct messages, Facebook Messenger App, WhatsApp, Email, and Texting)

See question 1 in the Youth Groups, Children & Young People section below

---

6. **How do we safeguard people from 'auto play' videos? I.e. when an inappropriate video automatically plays after watching a church video on social media**

Short answer: This isn't the responsibility of the church, as they don't control the autoplay feature. See below for links to education on how to use (and turn off) these features on YouTube and Facebook. For users aged 13–17 on YouTube, auto-play is turned off by default. If you're 18 or over, auto-play is turned on by default.

Resources:
Autoplay on YouTube
Autoplay on Facebook

[last updated Aug 2022]

---

7. **What is best practice for using TikTok as an individual?**

See question 14 and 15 of the Youth Groups, Children & Young People section

Youth Groups, Children & Young People

This section applies to church, circuit, district youth groups or other activities related to children and young people (predominantly under 18s) in an online space. The guidance here is partly an adapted and updated form of the Connexional Children and Youth social media guidance, partly links to external resources and professional advice, and partly our best practice recommendations to questions that aren't covered by the above.

You should contact your Church/Circuit Safeguarding Officer, District Safeguarding Officer or the Connexional Safeguarding Team immediately for advice if you have any safeguarding concerns about a child or young person, and also follow Methodist safeguarding policies, procedures and guidance.

1. **What are the best practices for leaders communicating with under 18s via electronic means?** (e.g. social Media direct messages, Facebook Messenger App, WhatsApp, Email, and Texting - this does not refer to offical church social media or best practices for online group settings like Facebook Groups or Zoom)

Short answer: Leaders must not communicate one-to-one with under 18s via personal social media profiles or email accounts (see more details under question 2 of the Individual Social Media Use section). Messages must be in a group format with more than one over 18 leader in the group or from a work account that multiple over 18 leaders have access to. Only children/young people who are known should be involved via communication in this way.

Longer explanation and other scenarios: Permission from the parent/guardian of any under 18 needs to be obtained before you can contact them. If the child is over 12 they are also required to sign the consent form. If the young person is 16 or above and living independently/is estranged from their parents then the form must be signed by the young person and a social worker/youth work/appropriate adult. These will need to be filled out annually.

Always conduct yourself the same way on the internet as you would face to face. Be aware of what you say and how you say it, as well as how it could be interpreted. Try not to use abbreviations, as these can sometimes be misconstrued. Never provide personal details of yourself, young persons or volunteers.

Do not communicate with young people outside of standard working day hours (9am – 5pm). The only exceptions to this would be if any evening activity is happening and a reminder needs to be sent beforehand or closing message afterwards.

Only communicate with a young person in a group context involving two or more leaders. If you are contacted in a private setting, do not reply. If their communication needs responding to, add another leader to your conversation in order to remain accountable. If you are contacted directly on a church social media account, alert the other admin or account holder that this has happened in order to remain accountable. Do not engage in conversation beyond responding to simple queries.

Any emails sent to multiple young people/parents should have their individual email addresses put into the BCC section so they won't be able to access each other's addresses. A second leader should be copied into email as a direct recipient or CC. Alternatively, send from an email address that multiple leaders have access to.

Leaders involved in children and youth ministry should only have under 18s mobile numbers if they have been given on the consent form as a means of communication.

If a young person contacts you and appears to need urgent help or appears to be at immediate serious risk, contact 999, social services or other relevant services, and inform your Church safeguarding office who may consult with the District Safeguarding Officer. If you are unable to contact the church/circuit safeguarding officer, please contact your District Safeguarding Officer.

Resources:

Consent form for communication with under 18s

[last updated Mar 2022]

---

2. **What is best practice guidance for using social media in a personal capacity as an employee, minister, volunteer, or in a leadership position?**

See answer under question 1 and 2 in the Individual Social Media Use section

---

3. **What consent and consent forms are needed to include identifiable under 18s in church videos, photos, audio, or live streams that will be used online?**

See answer under question 2 in the Consent Form section

---

4. **Should photos/videos of identifiable under 18s posted online in the past without correct permissions, sometimes having been online for many years already, be removed?**

See answer under question 2 of the Church Websites section

---

5. **What is best practice guidance around church youth Facebook Groups? (or any Methodist Facebook Group aimed at under 18s)**

Short answer: Groups that are specifically for under 18s should be made private, and in most cases only contain the young people linked with the church and official leaders. See the section on "Church Facebook Groups" for general best practice guidance on Facebook Groups. All admins of Facebook Groups for under 18s must be safer recruited and have a DBS check.

Longer explanation and other scenarios: The Group should always have two or more leaders as admins. It is important to note that their personal accounts will be the ones visible in the group when they post, so personal account privacy settings are very important. It doesn't matter who fulfils the role of admin in a group as long as they are over 18, and can be decided on a church by church basis. However, it is essential that they have been through the safer recruitment process. It is not appropriate to include a parent in a Youth Group Facebook Group, unless they are an official leader on behalf of the Methodist Church. Adults can communicate with under 18s in a public context, such as in comments of a church post on social media, or within a public church Facebook Group, however, within a closed Facebook Group it depends on the purpose. A dedicated Youth Group Facebook Group should be set to private, and if a young person leaves the church or youth group, or turns 19, they should ideally leave the group. However, this isn't a set rule, as it would be fine to have a closed Facebook Group for a wider purpose that contains a mix of adults and under 18s, as long as there are clear group rules, at least 2 or more admins, and there is good moderation taking place. In this context all communication between the under and over 18 year olds is being monitored.

[last updated Mar 2022]

---

6. **Can you have a Church Facebook Group that contains a mix of under 18s and adults?**

See answer under question 3 of the Church Facebook Groups section

---

7. **What are the best practices for hosting a Zoom youth group or meeting for all under 18 year olds?**

Short answer: Ensure there are at least two leaders, who have been recruited using the Safer Recruitment processes (references and DBS checks) in each virtual meeting (and make sure the leaders 'arrive' before the group does). You will need parental consent to include their child in any virtual meeting space and, for those under 16, the parents/carers will need to be the Zoom account holders and the link for the meeting should be sent to them. We also recommend that parents/guardians are asked to supervise the Zoom call. Do not record the meeting. In the settings for your Zoom meeting you should disable the one-to-one anonymous chat function so that participants cannot send private messages that are not seen by the wider group. You may also want to consider disabling screen share and only allowing this if needed for a particular activity.

Longer explanation and other scenarios:

It's important to note that Zoom's advice around under 16s using the platform is: "Children under 16 cannot create a Zoom account. A parent or guardian may, however, permit the child to use that parent or guardian's account with their supervision."

Contact the parents and carers of those under 16 via email or direct messaging, informing them of your intention to create a virtual meeting group. Seek their support and permission to do this. Explain how, when and where the meeting will be happening so everyone is clear about how it will take place.

Encourage parents/carers to talk with their children about these new arrangements. Let them know who they can contact if they have a question or concern. It is essential that they are on board and able to set boundaries that they feel are appropriate for their children whilst they are on the Zoom chat (eg. the parent might want the child to participate in the Zoom chat from a visible space in the house or, if the child attends the meeting from their bedroom, they might want them to leave the door open, or they might just want to check in with the child at the end of the meeting).

Ask parents/carers to complete and return **this consent form** before their child participates in a Zoom gathering. You can use the following text in your email for parents/carers, to offer an explanation of the expected supervision:

"Parents/carers we ask that you supervise* your child's use of the Zoom account and are aware of when, how and why they are using the account, ensuring that you keep the log in details and do not share this with your child. Each time your child wants to attend a session facilitated by your church or organisation. You should log them in for the session, do not give them the log in details. please ensure that you read and follow the Methodist Church guidelines outlined in our **Zoom Safeguarding policy.**

Zoom collects information about its users and has its own privacy terms and conditions to which members must adhere. Please review **Zoom's privacy terms and conditions** carefully before registering, and ask parents/carers to do so also.

The session leaders will ensure that they comply with the Methodist Church Safeguarding procedures and policies in the same way that they would if meeting face to face.

* By supervision we mean: The parent/carer holds the responsibility to log in to the Zoom meeting and agrees to not share the log in details. The parent/guardian is also responsible for logging out of the Zoom call at the end of a session and checking that privacy settings haven't been changed and their passwords are not saved. The parent/carer is to manage the Zoom account and to ensure that they are at home while the child or young person is attending the session. Where possible the child/young person should be in a communal space or in a room with the doors left open when accessing the session via their laptop, computer or other device.

Shortly before it is time for everyone to join in, send the Zoom link to the parents/carers of those under 16 years and directly to those who are 16 or above. As leader of the group you have control over when the video meeting starts and ends and no interaction can take place unless you have opened the space first or after you have closed it.

It is best practice to keep a log of your Zoom meetings. Who attended? How long did it last? Also include a brief description of what was covered and if any issues arose.

Resources
Virtual meeting youth groups, a step by step guide (Connexion)
Zoom guide for parents and carers (UK Safer Internet Centre)

[last updated Aug 2022]

---

8. **Can you have a Zoom meeting that contains a mix of under 18s and adults?**

See answer under question 5 of the Zoom & Video Conferencing section

---

9. **What is best practice in using the chat function in Zoom?**

See answer under question 3 of the Zoom & Video Conferencing section

---

10. **What is best practice guidance around church youth WhatsApp Groups? (or any Methodist WhatsApp Group aimed at under 18s)**

Short answer: See more details under the WhatsApp section

For groups with under 18s, the following guidelines and code of practive should be considered:

- Consent should be obtained from a parent or guardian for a young person to join a WhatsApp group.
- Groups for young people should be monitored by two adult group leaders who are safely recruited to the role and have appropriate DBS checks and safeguarding training.
- Group leaders should not contact young people on WhatsApp outside of the group chat.
- Group leaders should ideally use a church issued phone where this is possible.
- Other adults, including parents, should not be added to the WhatsApp group unless they are safely recruited to work with children and young people on behalf of the Methodist Church, with appropriate DBS checks and training.

[last updated Aug 2022]

---

11. Can a church WhatsApp group contain a mix of under 18s and adults?

See answer under the WhatsApp section

---

12. Can you have under 18s as admins of church social media accounts?

See answer under question 2 of the Church Social Media Accounts section

---

13. Can Church Social Media accounts follow, comment, or interact online with under 18s, either on their posts or your own posts?

See answer under question 7 of the Church Social Media Accounts section

---

14. What is best practice for youth groups or young leaders using TikTok in an official capacity?

Individuals are welcome to use TikTok personally (see below question 15 for online safety and privacy advice for TikTok). As a platform it's still unlikely to be appropriate or useful for a church to join TikTok in an offical capaticy, however, it might be suitable for young leaders, ministers, or pioneers to engage on TikTok, to reach those outside the church. If a large portion of your church youth use TikTok it might also be an appropriate space to have an official presence. Ideally, this should be by young people, for young people - given the main demographic on TikTok is still currently Gen Z (at the time of

written those aged 11-25 years old ish). TikTok is a video platform, and so all safeguarding guidance in this document related to recording and sharing video should be followed (see all questions in the Consent Form section). If a TikTok account is set up in an official capacity for a church or youth group, then all guidacnce in the Church Social Media Accounts section should be followed. Alternatively, if your TikTok account is set up as a personal space by a minister, young leader, or pioneer, then the guidance in the Individual Social Media Use section should be followed.

Resources:
Does my church need to be on TikTok? (Church of England blog)
Four positive ways churches can use TikTok (article)
Tips for using TikTok for churches (article)
How vicar's TikTok meant for seven teenagers reached 1.7 million (Church of England)
Parents guide to TikTok
Staying safe on TikTok - Privacy and safety tips from TikTok

---

15. Useful links to online safety resources:

See below a range of external signposted links that may be of use to organisations, parents, and young people.

Useful links for churches, schools, and organisations:

- Advice for planning online performances (although this says for schools there is useful advice for anyone who is planning to do this).
- Teaching online safety in schools This government guidance outlines how schools can ensure their pupils understand how to stay safe and behave online as part of forthcoming and existing curriculum requirements.
- Lesson plan toolkits from Childnet (KS3) - Lesson plans and video content covering cyberbullying, sexting, peer pressure, self-esteem, online pornography, healthy relationships and body image for 11-14s
- Step Up, Speak Up! From Childnet - A practical campaign toolkit to address the issue of online sexual harassment amongst young people aged 13 – 17 years. Resources, guidance and information for professionals to raise awareness of online sexual harassment amongst young people and to increase reporting
- The Well Learning Hub (Methodist Church) - equipping and support those who work with children, young people and families in the church. Indlcuing Methodist social media guidelines

Useful links for parents:

- Childnet has developed guidance for parents and carers to begin a conversation about online safety, as well as guidance on keeping under-fives safe online
- Parent Info is a collaboration between Parent Zone and NCA-CEOP - support and guidance for parents and carers related to the digital world from leading experts and organisations
- National Society for the Prevention of Cruelty to Children (NSPCC) - guidance for parents and carers to help keep children safe online
- UK Safer Internet Centre - tips and advice for parents and carers to keep children safe online - you can also report any harmful content found online through the UK Safer Internet Centre
- Inclusive Digital Safety Hub and Online Safety Hub, created by South West Grid for Learning in partnership with Internet Matters - support and tailored advice for young people with additional learning needs and their parents or carers
- Internet Matters - a one-stop-shop for parents: online issues, advice by age, setting controls, guides and resources
- Thinkuknow by the National Crime Agency - Child Exploitation and Online Protection command (NCA-CEOP) - resources for parents and carers and children of all ages to help keep children safe online
- Get Safe Online - free, impartial online safety advice on safeguarding children when they are online. Find advice on many topics including gaming, cyberbullying and social media.
- Google Safety Advice - helping families navigate tech, such as setting parental controls, tips for parents, and activities for families
- Parents guide to TikTok - an overview of TikTok and the many tools and controls built into the product to keep the community safe. The guide also provides general information on common internet safety concerns.
- Zoom guide for parents and carers (UK Safer Internet Centre)

Useful links for young people:

- Childline - If you are experiencing bullying or other unwanted online contact, or if you want information on internet safety
- Childnet has advice and information for young people aged 11-18 on where to go for help online

- Thinkuknow help for 4-7 year olds, 8-10 year olds, and 11-18 year olds.
- UK Safer Internet Centre - resources for 11-19s: Here you will find films, games, quizzes and advice to help you to use the internet safely, responsibly and positively
- Staying safe on Instagram - Privacy and safety tips from Instagram
- Staying safe on Facebook - Privacy and safety tips from Facebook
- Staying safe on YouTube - Privacy and safety tips from YouTube
- Staying safe on TikTok - Privacy and safety tips from TikTok