

Staying Safe Online: Safeguarding Top Tips for NPNP *in the Sheffield District.*

Digital and social media platforms offer valuable opportunities for NPNP projects to connect with communities, share stories, promote activities and build relationships. However, our online presence should always reflect Methodist values of **respect, care, inclusion, accountability and Christian witness**.

The Methodist Church has published Social Media Guidelines and safeguarding guidance for churches, circuits, districts, ministers, employees, volunteers and individuals engaging online. NPNP projects are encouraged to familiarise themselves with this guidance and apply it consistently in all online activities.

<https://www.methodist.org.uk/for-churches/digital-church/social-media-guidelines/>

While the Methodist Church provides guidance based on our values and safeguarding responsibilities, it is important to remember that every social media platform also has its own rules, community standards, safety features and reporting processes.

NPNP projects, church leaders, volunteers and administrators should familiarise themselves with the guidance provided by the platforms they use, such as Facebook, Instagram, X, TikTok, YouTube and WhatsApp.

Most platforms provide:

- Privacy and security settings.
- Community standards or acceptable use policies.
- Reporting tools for bullying, harassment, abuse, hate speech and inappropriate content.
- Blocking, muting and restricting functions.
- Guidance on protecting children and young people online.
- Advice on recognising scams, fake accounts and misinformation.
- Account recovery and security support if an account is compromised.

Good Practice for NPNP Projects:

- Review platform safety settings regularly.
- Ensure all administrators know how to report concerns.
- Make use of moderation tools to help maintain a safe online environment.
- Keep up to date with changes to platform policies and safety features.
- Encourage participants, volunteers and church members to learn how to use the safety tools available to them.

The Methodist Church's guidance should be used alongside, not instead of, the safety guidance provided by social media companies. By following both, NPNP projects can create safer, more welcoming and better-managed online communities.

Remember: If behaviour online is abusive, threatening, harassing or otherwise concerning, use the platform's reporting tools and follow Methodist safeguarding procedures where appropriate.

1. Think Before You Post

Online content can be permanent, even if deleted later.

Before posting, ask:

- Is it true?
- Is it respectful?
- Is it appropriate?
- Do I have permission to share it?

- Does it reflect Methodist values?

Remember that posts, comments, photographs and messages can be copied, shared or screenshotted by others.

2. Respect Privacy and Confidentiality

Protect both your own privacy and that of others.

Good Practice:

- Obtain appropriate consent before sharing photographs, videos or personal stories.
- Never share confidential information online.
- Avoid posting personal contact details, addresses or location information.
- Consider whether information could unintentionally identify vulnerable individuals.

3. Create Safe and Secure Church Accounts

Official NPNP project and church social media accounts should be linked to a church-owned or role-based email address rather than an individual's personal account.

Recommended Setup:

1. Create a dedicated project or church email account.
2. Use this email account to register social media platforms.
3. Appoint at least two authorised administrators.
4. Use administrator permissions rather than sharing passwords.
5. Enable Two-Factor Authentication (2FA).
6. Store account details securely.
7. Ensure access can be transferred when roles change.

4. Protect Your Accounts

Stay Secure:

- Use strong, unique passwords.
- Enable Two-Factor Authentication.
- Review privacy settings regularly.
- Keep devices and apps updated.
- Limit administrator access to authorised individuals only.

Be cautious about sharing:

- Home addresses
- Phone numbers
- Travel plans or holidays
- Personal information about others

5. Engage Respectfully Online

Social media should be a place where everyone is treated with dignity and respect. When personally criticised, avoid responding in kind.

Do:

- Listen respectfully to different viewpoints.
- Engage thoughtfully in discussions.
- Respond calmly and graciously.
- Remember there is a real person behind every comment.

Don't:

- Post abusive, hateful or threatening content.
- Engage in personal attacks.

- Share inflammatory or misleading information.
- Respond angrily when challenged.

6. Managing Trolls and Hostile Behaviour

Online trolls are often seeking attention, conflict or disruption rather than genuine conversation.

Good Practice:

- Pause before replying.
- Avoid emotional responses.
- Distinguish between genuine criticism and deliberate provocation.
- Use platform tools to mute, block or report users when appropriate.
- Report abusive, threatening or harassing behaviour.

7. Welcome Constructive Feedback

Constructive feedback can help projects learn, improve and strengthen relationships within the community.

A Positive Approach:

1. Thank people for raising concerns.
2. Listen carefully to the issue.
3. Respond politely and factually.
4. Avoid becoming defensive.
5. Move detailed discussions offline where appropriate.
6. Learn from valid criticism.
7. Apply moderation rules consistently if behaviour becomes abusive.

8. Spotting Scams and Misinformation

Churches and community projects can sometimes be targeted by scams.

Be Alert To:

- Requests for money or gift cards.
- Messages claiming to be from ministers or church leaders.
- Urgent requests for passwords or personal information.
- Suspicious links or attachments.
- Stories that cannot be verified.

Always check information before sharing it and encourage others to do the same.

9. Establish Clear Group Rules

Every church or NPNP social media group should have clear and visible rules.

Group rules help:

- Promote respectful discussion.
- Reduce bullying and harassment.
- Protect vulnerable people.
- Support administrators when moderating content.
- Create welcoming online communities.

10. If a Social Media Account Is Hacked

Act quickly:

- Change passwords immediately.
- Enable or strengthen Two-Factor Authentication.
- Remove unauthorised administrators.
- Log out suspicious sessions and devices.

- Take screenshots and keep records of activity.
- Remove unauthorised posts or messages.

Notify:

- Church or project leadership.
- The safeguarding officer if safeguarding information may have been accessed.
- Those affected where appropriate.

Following recovery, review security arrangements and strengthen procedures to prevent future incidents.

11. Healthy Online Boundaries

Appropriate boundaries are essential, particularly when communicating with children and young people.

Good Practice:

- Use approved church or project communication channels.
- Avoid unnecessary private messaging from personal accounts.
- Ensure communication remains transparent and accountable.
- Follow local safeguarding procedures and Methodist guidance.

Online interactions should be subject to the same safeguarding standards as face-to-face activities.

12. Wellbeing and Digital Resilience

Being online can sometimes be demanding.

Remember:

- You do not have to engage in every discussion.
- It is acceptable to leave conversations that become unhealthy.
- Taking breaks from social media is good self-care.
- Seek support if online interactions are affecting your wellbeing.

Staying safe online is everyone's responsibility. By acting thoughtfully, respectfully and responsibly, NPNP projects can help create positive digital spaces that are welcoming, inclusive and safe for all.