

High Street Presbyterian Church Online Safety Policy

Aim

The church recognises that technology can be a positive tool when well used, especially in youth ministry. Our aim is to support the best practices when using technology, keeping everyone as safe as possible.

Our Church Website

The session will designate a site administrator who will have overall responsibility for

- Adding and removing material from the website in a timely manner
- Ensuring the online environment is safe and secure
- Providing information to congregational members and site visitors
- Promoting the mission and ethos of the church

At times, other administrators may be approved to provide material for the website. The website will be under frequent review of Kirk session, whose decision over inclusion of content will be final.

Content

The administrator will ensure that

1. All content is reflective of the congregation mission and ethos
2. Any content which the session deem contrary to church doctrine or ethos shall be removed immediately
3. None of the content posted breaches copyright or can be claimed to be slanderous or libellous
4. Content will conform to safeguarding requirements- eg. permission will be sought for photos, or stock photos used for children's groups.
5. Content is kept up to date
6. External links open in separate browser windows and are clearly labelled
7. Privacy is maintained for all congregational members by encouraging the use of the central church email address for correspondence
8. The church website will not be used to send unsolicited email, or pass on information to a third party.
9. All material used on the website is from a reputable source with suitable licencing and fees paid if necessary
10. The website should be password protected with only a limited number of people able to access . However at least two people should have knowledge of the password at all times.

Internet and online communication

Access to the internet

Like most churches, we have internet access which is used for a variety of purposes throughout the church. While use of such technology is of benefit, we must be vigilant and alert to the possibilities for misuse and the subsequent harm that could result.

Use of computers

1. Computers/ laptops should only be used by those who have permission to use them and for the purpose they were intended.
2. Passwords should not be shared with others without permission
3. No church laptop should be removed from the church premises.
4. When working with children/young people, material should be prescreened to ensure it is suitable for the age group
5. Appropriate firewalls/ anti virus software and if needed child monitoring software should be installed.
6. When working with children, always ensure the computer is open for all to view.
7. Do not download any material for your own personal use
8. Any material deemed to be offensive will result in removal of computer privileges and possible reporting to session
9. Any concerns about material that may be deemed a safeguarding risk should immediately reported to the designated person.
10. No material should be downloaded illegally

Communication

When properly used, digital communication is a fast and effective tool, particularly in youth ministry. However leaders should never engage in **personal** conversations with young people under the age of 18 through any form of digital communication. Nor should they accept friend requests from young people of this age.

Group accounts such as WhatsApp are used to communicate by most organisations. If using such a group :

1. Access should only be by invite or request
2. Only one group should be created by the leader in charge, with at least one other leader .
3. Messages should be seen by all
4. The leader in charge should closely monitor conversations, memberships and content
5. Leaders should be aware that the legal minimum age is 13 for such a site. This may mean that some you get children will be left out, or will try to join even though they are not the correct age.
6. Some children/ young people may choose to opt out of the groups. Leaders must ensure they do not miss out on shared information and must find another way to communicate with them
7. Care should be taken when posting photographs to ensure that all permissions have been obtained. Reminders may need to be given for others posting photos and photos taken down
8. Comments written on social media must be treated the same as face to face, so any disclosures online must be reported to the Designated person in line with the safeguarding policy.
9. A leader wanting to send an individual message to a child- such as a good luck message for exams- should do this via the child's parents/ guardians

Use of mobile phones

There is no one size fits all for the use of mobile phones within the church. Each group is expected to have it's own guidance which it will include within it's risk assessment.

The general guidance is:

1. Mobile phones should be either switched off or on silent
2. Photographs should not be taken without consent
3. If you need to take/ make a phone call, go somewhere where you will not be overheard
4. In a children's/ youth group, have clear guidance on what is and isn't allowed.

Further guidance on technology and the signs of online abuse can be obtained from the PCI safeguarding website.

Adopted by the Kirk Session of High Street Presbyterian Church on 26th May 2026.

Minister: Jimmy Warburton

Designated Person: Audrey Gordon