

As we navigate the COVID-19 situation with our congregations, and work to stay connected through digital platforms, it is important to consider best practice to keep people safe online, especially the vulnerable within our congregations.

A Child or Young person is someone under the age of 18.

LIVE STREAM

When using live stream, ensure that no images of Children or Young People are included if you do not have permission for their image to be online, or if there is a custody issue that could endanger them if they were seen online.

Do not use live chat with Children or Young People. When streaming a service, anyone outside your organization can engage with live chat and connect with those involved.

ONLINE GROUP MINISTRY

Consider the privacy requirements of gathering people's data to an online platform. How is this data stored and used by the platform? Who has access to this information now and in the long term?

For any group involving Children or Young People, consent must be obtained from a Parent or Guardian for the child or young person to be involved. Any group involving children 12 years or younger must be set up using only a Parent/Guardian's email and login, and login-in details must not disclose a child's full name. Groups involving teenagers must ensure that Parents/ Guardians consent to a young person's email being used as a login. Links to any online platform should not be in the public domain, but sent only to those invited to the group. Groups involving children 12 years or younger should have their Parent/ Guardian present throughout the online connection.

Educate people around online etiquette and expectations as well as protecting personal and private information. This is particularly important for Children and Young People.

Disable private chat functions through these platforms, particularly for any group involving Children or Young People.

Groups involving Children or Young People should have two unrelated team members to host and moderate the group, and the session should be recorded for transparency and accountability. Ensure recorded content is not stored on private computers, but stored securely by your church. If it is only possible to have one team member hosting a group, ensure that the online connection is set up to commence only when there is more than one Child or Young Person connected.

It is advisable that no screen shots of groups involving Children or Young People be taken. If a screen shot is taken for use on church social media platforms, ensure there is consent to use the images of the Children and Young people involved, and have clear guidelines around the retention of such images on private devices, and who can post such images to social media platforms.

Ensure you comply with the terms of any social media platform. For example, Facebook and Instagram have a minimum age of 13 years for someone to have a personal account. Be aware, that if a child uses another person's profile to engage with the platform you are using, any comments they make using this platform will appear to come from the person holding that account.

- Encourage Parents/Guardians to educate their children about online safety. The National office of eSafety and the NSW Department of Education have informative and useful resources, including on Facebook and Instagram. The links to their websites are:
 - <https://www.esafety.gov.au/>
 - <https://www.digitalcitizenship.nsw.edu.au/>

- Ensure all your church knows how to report any concern or allegation of inappropriate online interaction and that all legal reporting requirements are followed. Contact the Safer Churches helpline for advice and assistance: 1800 070 511.