Appendix 5

Cornerstone Evangelical Church

Online Safety Policy

Online Safety definition:

Online safety is the collective term for safeguarding involving the use of electronic devices and applications to communicate and access the Internet; often referred to as Information and Communications Technology.

The church has adopted good practice to ensure that modern technologies are used safely and responsibly in order to protect young people and their workers. This policy reflects communication between Cornerstone Evangelical Church (CEC) workers and children (those under 18 years of age).

Electronic communication should not be made with children under 13 years of age

Expected ways of communicating with young people online

- Meeting as a group through an online video chat platform
- Connecting with individuals and groups through messaging software
- Broadcasting activities or video on social platforms
- A video call with a young person and two approved youth workers

Online platforms that have been agreed for use by CEC

YouTube(CEC channel)
Instagram(for Cornerstone Youth (CY) group. Admin – Children and Young People's worker)
Facebook
Twitter
Zoom
Email
WhatsApp
Churchsuite

Consent and Permissions

Electronic communication

- Written permission should be sought annually from parents/guardians and from the child/young person themselves before using electronic communication methods for church purposes, via the general consent form.

Appendix 5

Photographic images and videos online

- The Children and Young People's worker must ensure that parents are given the opportunity to consent to or refuse permission for their children or young people to be photographed by the church and used for publicity. This should be made annually via the general consent form.
- Images will only be used for the specific purpose for which permission was sought for and how the image will be stored if not destroyed. If the intention is to use an image on the internet this must be clearly stated, and further permission must be acquired if an image is to be used in a way not originally stated.
- The church will not upload images, video or any other media of children and young people to the internet or allow photographs of children and young people to be made available for downloading / copying or printing, without specific permission from the child/young person and parent/guardian.
- Live streaming of events must be clearly advertised in advance and where children are involved permission should be sought in line with the photographic guidelines.
- There may be occasions where an individual e.g., a parent may wish to take photographs to record parts of a church service and in those circumstances, this will be allowed providing no-one objects. In such circumstances the decision of the meeting leader is final. The leader of the meeting may ask that images are for private use only and not shared on social media
- Children and young people choosing to photograph or video and upload this content themselves on their own devices to their own online accounts is not the Church's responsibility.

General points

- Photographs that include children will be selected carefully and CEC will endeavour to prevent children from being easily identified.
- Children's full names will not be used on the website in association with their photographs.
- When recording regular church services for later online viewing, every effort will be made to minimise the incidental recording of children and young people.
- Use of images will reflect diversity of age, ethnicity, and gender of the activity.

Online communication guidelines

- Ensure the CEC domain name/logo appears with every Internet post made by a church computer user. Any user will then be viewed as a representative of your church/organisation while conducting business on the Internet.

- Electronic communication should primarily be used for factual/administrative matters.
- Electronic communication between a church employee or worker for church purposes and a child/young person, should be copied to the parent/guardian or another CEC employee and not solely to the young person.
- There may be occasions where it is appropriate to print a record of communications.
- Any texts or conversations raising concerns should be passed to the Safeguarding Coordinator
- Email should only be used to communicate specific information. (e.g. times and dates of events). It should not be used as a relationship building tool.
- Maintain a log of all electronic contact with individuals or groups by not deleting electronic communication including emails, messaging and texting.

- Where possible, CEC workers should use equipment provided by the church/organisation to communicate with children, rather than personal devices.
- Electronic communication with children is advised to take place between the hours of 9am-5pm where possible. Where working with children outside normal office hours workers should seek advice from their Ministry lead but there should be no electronic communication after 9pm.

Social Media guidelines

- All social media interaction between workers (paid or voluntary), and children under 18 shall be limited to monitored/administrated groups.
- Text and any other media posted shall be subject to the **acceptable use** policy
- Social media shall be used for group information purposes only and comments turned off
- Any safeguarding concerns/allegations arising from social media shall be referred onto the safeguarding co-ordinator.
- Respect the minimum age requirements for video chat enabled platforms and Apps.e.g.13 years for Facebook
- Workers should ensure their privacy setting ensure the highest levels of security in order to restrict children being able to see any more than what is relevant to communication within the group
- All social media groups should provide links to statutory authorities such as CEOP, to enable children to report online abuse.('Click CEOP' is a resource for children and young people worried about online abuse to report concerns).

Online video chat guidelines

- Never share the meeting link publicly, only directly with the parents of children or with the people in your community group etc.
- Ensure the meeting has a password and only share it directly with parents or the people your meeting is for.
- Ensure that waiting rooms are set up and that people can only join when permitted by the host and ensure you do not admit any people unless you are **sure** who they are.
- Ask all attendees to set their display name to their real, full name so that you can be sure who they are so you can allow them to enter the meeting.
- Ensure you meet all safeguarding child/volunteer ratios, just as you would with in-person meetings.
- For children's meetings, turn off all private chat functions.
- Avoid using breakout rooms.
- Disable screen sharing for anyone apart from the host.
- Obtain written consent from parents (can be from their personal email) for all meetings, making clear the time and what the meeting purpose is. If the meeting is regular, one permission is sufficient.
- Always contact children through their parents, never directly and ensure they are using parents accounts under supervision.
- Ensure parents and children are aware the child should be supervised or visible in a shared space for the duration of the call.
- Keep an attendance record of all meetings time, people and content and report to a centrally, as for an in-person meeting

Online video chat guidelines for parents/guardians

- Ensure your child stays in a shared space while they are using the platform and remain under your supervision at all times.
- Your child should use your own account, and you are responsible at all times for their use of the software.
- Never share the link with anyone else, including with friends or other church families. The links are sent directly to only those who have registered in advance, granting consent, and agreeing to the guidelines.
- Provide written consent to the leaders before allowing your child to use the platform for ongoing or one-off sessions.

Code of Conduct for Church Workers working online with children

- Generally, maintain good and open relationships with parents and carers regarding communication with them and their children.
- Use an appropriate tone: friendly, but not over-familiar or personal.

- Be warm and friendly, but do not suggest or offer a special relationship.
- Be clear and explicit about information that you need to share; don't abbreviate or short-cut your communications.
- Be circumspect in your communications with children to avoid any possible misinterpretation of your motives or any behaviour which could be construed as grooming.
- Do not share any personal information with children, or request or respond to any personal information from a child other than that which might be appropriate as part of your role.
- Only give personal contact details to children that are within the public domain of the church / organisation, including your mobile telephone number.
- Respect a child's right to confidentiality unless abuse/harm is suspected or disclosed.
- Only contact children for reasons related to the work of the church/organisation

Acceptable Use Policy

- Where access to the internet is provided on the church's devices, or on devices owned by an individual via Wi-Fi on CEC premises, we will exercise our right to monitor usage which includes access to websites, interception and deletion of inappropriate or criminal material or unlawfully copied text, video, images or sound.
- Wi-Fi Access will be via a secure password that will be changed regularly.
- Social media groups must be used in compliance with the church's policy on social media.

Children and Workers should not:

- Search for or download pornographic, racist or hate motivated content.
- Illegally copy or play copyrighted content where permission has not been given.
- Send, request, or display offensive messages or pictures.
- Harass, insult or bully others.
- Access the internet using another person's login details.
- Access, download, send or receive any data (including images), which the church considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.

Sanctions for violating the acceptable use policy in the opinion of the church may result in:

- A temporary or permanent ban on internet use.

- Additional disciplinary action in line with existing practice on inappropriate behaviour.
- Where applicable, police or local authorities may be involved.

Parent /Carer Agreement

As the parent/guardian of _____ I declare that I have read and understood the Online Safety acceptable use policy for **(insert church name)** and that my child will be held accountable for their own actions. I understand that it is my responsibility to set standards for my child when selecting, sharing and exploring online information and media.

Child/YP Agreement
I understand the importance of safety online and the church guidelines on acceptable use.

I will share any concerns, where I or another person may be at risk of harm with the safeguarding coordinator or a trusted adult.

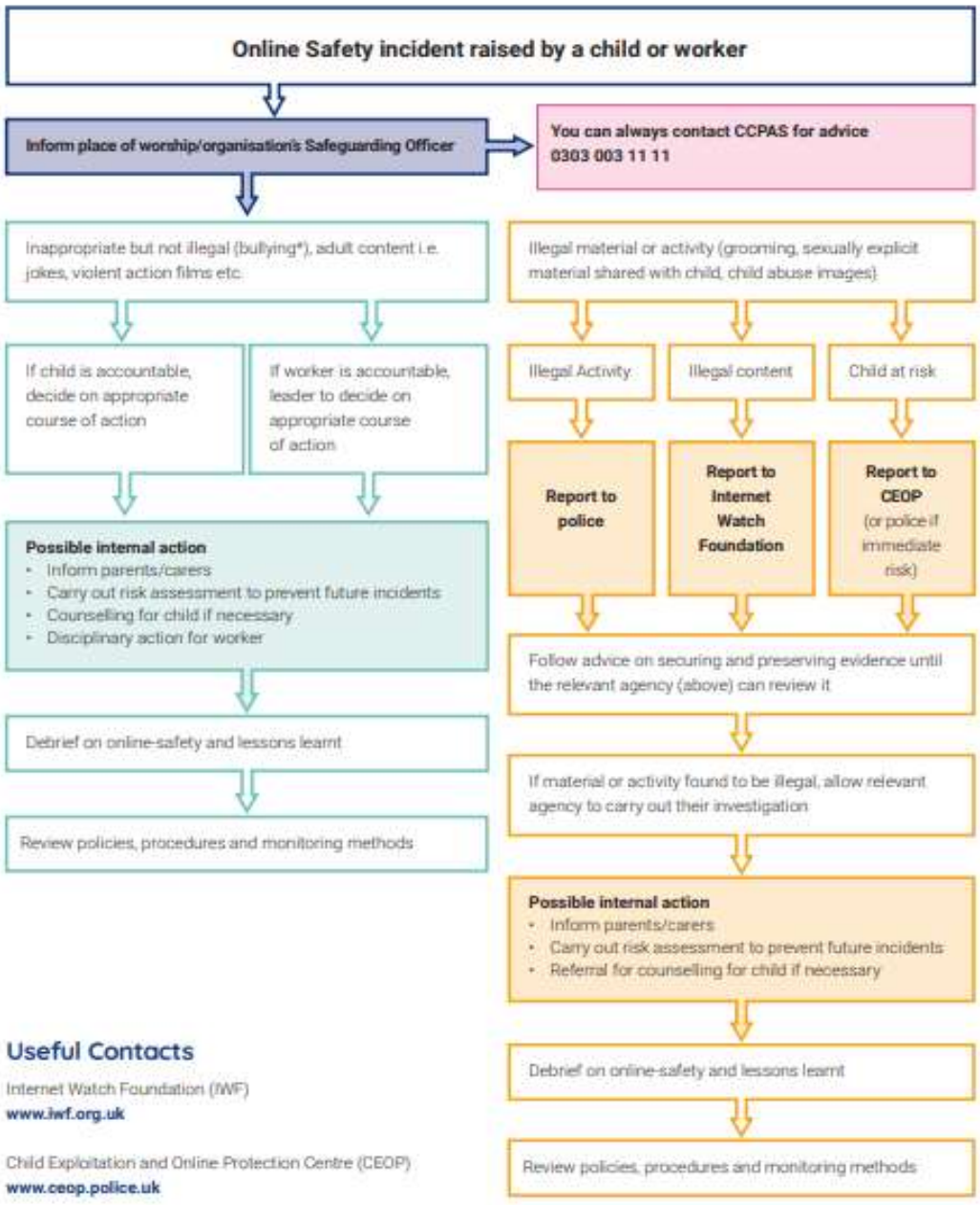
Child Name (Please print)	**Child Signature**	**Date**
Parent/Guardian (Please print)	**Parent/Guardian Signature**	**Date**

Responding to Online Concerns

Appendix 5

Online Safety Flowchart

thirtyone:eight
Creating safer places. Together.



Useful Contacts

Internet Watch Foundation (IWF)
www.iwf.org.uk

Child Exploitation and Online Protection Centre (CEOP)
www.ceop.police.uk

(*) Some forms of bullying or content may be illegal – see Malicious Communications Act 1988, Obscene Publications Act. For extreme pornography – Criminal Justice and Immigration Act 2008, etc.