Appendix 11: Online and Digital Safety

Young people and many adults use smartphones and tablets as their preferred means of communication. The ease and exclusive nature of these devices make them mediums for entertainment, communication, information and sadly abuse. All those working with children and adults should remain vigilant to signs of abuse through these mediums. Below are the guiding principles to be followed when communicating with children or adults at risk:

Policy guidelines for Church Workers/Volunteers

- 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. Clear and unambiguous language should be used.
- 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. Keep the content of the communication appropriate to the subject.
- Ensure all communication is in a group context.
- Only give personal contact details to children that are within the public domain of the church / organisation, including your mobile telephone number.
- If children want you to have their mobile phone numbers, e-mail addresses or similar, and communicate with them this way, make sure that their parents know and have agreed.
- Only make contact with children for reasons related to the work of the church/organisation and maintain a log of all electronic contact with individuals or groups including messaging and texting.
- Establish an agreed duration for conversations with children and a curfew for instant messaging, i.e. not between 10pm and 7am.
- Where possible employees should seek to use equipment provided by the church/organisation to communicate with children.
- Respect a child's right to confidentiality unless abuse/harm is suspected or disclosed.
- As far as is possible, ensure your church/organisation domain name/logo appears with every Internet post made by a church computer user. Any user may thus be viewed as a representative of your church/organisation while conducting business on the Internet.
- 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.
- When sending an email or text to young people or adults at risk, workers should copy it to a third party adult within the church/department to maintain accountability.
- Email history should be kept and dated.
- When using email/internet for communication with children, it is advised that it should take place between the hours of 9am-5pm. It is advised that there should be no email communication after 9pm.
- Use of Zoom and any other web camera or visual communication via the internet is generally not permitted.
- Workers should refrain from using such methods on a one-to-one basis. It can be used for conference calls and is considered appropriate if a project or group uses a web camera in a group environment for project purposes, and has clear aims and objectives for its use.

Social Media Policy

- On social networking sites such as Facebook the presumption must be that adult leaders are not added as friends on a young person's site. Leaders should instead use a 'role' profile i.e. 'Youth Leader' that is held generically between the leaders.
- 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
- All interaction on social media groups shall be recorded for safeguarding purposes
- Any private messages shall be recorded for safeguarding purposes
- Any safeguarding concerns/allegations arising from social media shall be referred onto the safeguarding co-ordinator.
- All users of social media must be above the minimum age limit i.e., 13 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 Child Exploitation and Online Protection (CEOP), to enable children to report online abuse.

Consent for photographic images and videos online

- Photographs that include children will be selected carefully and will endeavour to prevent children from being easily identified.
- Exercise caution when sharing identifying information/images of children on any internet site. Do not name the individual child without consent from the person with parental responsibility.
- Permission will be sought before any images are taken or displayed and images will only be used for the specific purpose for which permission was sought 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.
- Do not place children's profiles or personal details on a site without written consent of the person with parental responsibility.
- Use of images will reflect diversity of age, ethnicity and gender of the activity.
- 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.

Legislation allows for images of anyone in a public place to be published as long as the photography is not intrusive. Extra care should be taken not to capture children or adults at risk in situations that highlight vulnerabilities.

Before using a photograph/film of activities involving minors (under-16s), their consent and the written consent of a person with parental responsibility for them should be obtained. This must specify for what purposes the photograph/film will be used and how it will be stored if not destroyed. A sample consent form can be found in Appendix 11(b).

Acceptable Use Policy - (This can be included with consent/registration forms for children and young people with a request for acknowledgement by both parent and child)

Ensure that any of the church's electronic devices used by children and young people for accessing websites employ security controls.

Regular checks should be undertaken to identify and block any improper use of digital equipment or social media.

- Where access to the internet is provided on organisation devices or devices owned by an individual via WiFi, we may exercise the 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.
- WiFi Access will be via a secure password that will be changed quarterly.
- Social media groups must be used in compliance with **(insert church name)'s** policy on social media.
- Administrative control should be put in place and regularly monitored on all devices that are owned by the church.
- Involvement with any online forums should be moderated.

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 **(insert church name)** considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.

Any form of communication received which causes concern should be saved and passed onto the Designated Safeguarding Lead.

Sanctions for violating the acceptable use policy in the opinion of (insert church name) may result in:

- A temporary or permanent ban on internet use.
- Additional disciplinary action in line with existing practice on inappropriate language or 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/Young Person 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**