# APPENDIX 12: 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:

## Working with Children

**Requirements for Church Workers/Volunteers:**

- 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 avoid suggesting or offering a special relationship.
- Be clear and explicit about information shared; avoid abbreviating or short-cuts in 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.
- Avoid sharing 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 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.
- Only send emails 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. For example, publishing or broadcasting images of looked-after children may place them or others in danger in cases of abuse or domestic violence.

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 13(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/Guardian Agreement**

As the parent/guardian of [name of child], 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.

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

## Working with Adults at Risk

We are all vulnerable at certain times of our lives, depending on our circumstances and life events. When thinking of those more at risk than others, this could include a wide range of people e.g., those with physical disabilities or illnesses, care leavers, people with mental health difficulties, those with addictions, homeless people, abuse survivors, those in poverty, ex-offenders, ex-service personnel, minority groups, etc.

Despite the risks, we want to be online. We want all the benefits – the connections, the cost savings, the opportunities, the knowledge, the learning, the entertainment. For anyone with vulnerabilities or additional needs, the internet brings possibilities to combat isolation, join communities of interest, manage medical conditions, access self-help and overcome myriad barriers they may face in the physical world. For homeless people, internet access via a smartphone can be a lifeline to the world – the key to socialising as well as accessing services.

The internet can give vulnerable adults a wide range of options and tools to manage their lives and keep in contact with people. However, it can also expose them to abuse and crime.

**Internet crime**

Some fraudsters rely on the internet to commit crimes. The range of internet crime is growing, and it is important that adult at risk protected. Examples of internet fraud can include:

- bank and cheque card fraud
- business directory fraud
- charity donation fraud
- government agency scams
- health scams
- identity fraud
- online shopping fraud
- plastic card fraud.

It is important to use reputable internet sites. Find out more at getsafeonline.org.

**Tips**

It is a good idea to think about safety when using the internet, using some simple techniques can help protect your use of the internet and social media. Below are some tips to stay safer online.

**Security**

You should:

- install security software keep most viruses out
- get updates to reduce the ability of hackers and criminals to access to your data
- use complex passwords with no personal connection
- use encryption to stop others looking over your communications
- change your password regularly.

**Social media**

You should:

- take your phone number, address and date of birth off social media
- change your passwords if someone could guess them
- back up your data
- make sure you know who is using your computer
- check your privacy settings
- be careful what personal pictures you use and share with others
- only accept social networks from people you know and trust.

**Shopping online**

You should:

- take care with smaller, unknown retail sites
- make sure there is a secure symbol, usually a padlock when making a payment
- look out for poor spelling, grammar or anything unusual
- check there is a postal address, by law all traders must provide this
- use a credit card to pay, comes with insurance for purchases over £100.

**Mobiles and other devices**

You should:

- keep your phone well-hidden because they are easily stolen
- tag your device and battery with an ultraviolet marker pen with your name and contact it will make recovery more likely if lost or stolen
- use key pad lock
  use a password or pin
- register your device
- record your serial number which will help you report if your phone is lost or stolen
- insure your phone in the event of theft or damage
- restrict alternative Wi-Fi connections which can be a security risk
- block expensive calls and texts by phoning your provider.

For more help, contact ActionFraud or getsafeonline.org.

**Responding to risk**

There are various steps you can take to help prevent and respond to these risks:

Support the person to keep themselves safe online e.g., can you use existing educational materials? Technical settings (blocking, filtering, passwords etc.) may be appropriate. Discuss the kinds of online activities which would be illegal, inappropriate, or break an app's terms & conditions. Are they informed about their online rights? Where would they go for help if they needed it?

Look to your own and others' roles: how can you best support the person to exploit the benefits of the internet whilst managing the risks? How much do you (or someone else in their environment) need to be a positive part of their online experience (within professional boundaries)? You may find our resources for parents and carers useful.

Check your organisation has sufficient risk management policies and processes in place – look for resources specific to your organization.

## Responding to online harm

You may be managing a concern which has occurred online. This may be where you have become aware of harm through a digital service your organisation runs, where a member of your team sees harm online or it has been shared with you online. It may also be a situation where a member of your team has used your IT systems to perpetrate harm.

You may consider:

- **Where the concern is on a social media platform:** you should flag and report the concern on the third party platforms own community reporting systems (e.g. Twitter, Facebook, LinkedIn). These vary by platform and may depend on your administrator rights.

- **Where the concern is about child sexual abuse pictures and videos (including non-photographic images):** report to the Internet Watch Foundation.

- **Where you are concerned a child is being sexually abused or groomed online (including an unknown person communicating with a child for sexual purposes):** report to National Crime Agency's (NCA) Child Exploitation Online Protection (CEOP) Command. If you have already reported your concern to your local statutory service, including the local Children's Social Care or the Police, you do not need to make a report to CEOP.

- **Where intimate images or videos have been shared:** sometimes called "Revenge Porn", this includes sharing intimate images, either on or offline, without their consent with the intention of causing distress. This can also include threats to share intimate images; webcam blackmail ("sextortion") and upskirting. Report to the Revenge Porn Helpline

- **Online material promoting terrorism or extremism:** this includes articles, images, speeches or videos that promote terrorism or encourage violence; websites made by terrorist or extremist organisations and videos of terrorist attacks. Report to the Home Office

- **Other forms of online harm:** you may become aware of a wide range of harmful and distressing activity online including abuse, bullying or harassment or content which is violent, features self-harm or suicide or is pornographic. Report to the Report Harmful Content website.