1.1 Introduction

The digital world has now become part of everyday living, with the ways that we are able to access content online are changing considerably. This presents positive opportunities to support education, aiding creativity and self-expression. Conversely, this also poses a number of risks including cyber bullying, online grooming and identity theft.

When communicating via the internet and mobile phones, people can feel less wary and talk about things far more openly than they might when communicating face to face. Children and adults need to be educated on the safe use of mobile and internet communications.

1.2 Why online safety?

In the past, safeguarding has mainly revolved around the running of children's activities or events within church premises. Today, however, in addition to traditional activities and forms of communication, safeguarding includes online interaction.

Churches should, therefore:

- encourage children to stay safe online and direct them to age appropriate guidance
- ensure access to the internet on their premises is as safe as possible
- provide workers with policies and procedures for safer online communication with children

1.2.1 Myths about the internet

There are many myths surrounding the internet and how children, in particular, make use of it. In order to increase their own understanding, and to enable them to support children, parents, carers and workers to stay safe when online, it is important that all churches are aware that these myths exist. Myths include:

Myth: Young people are now so 'net savvy' and adults are almost always technologically incompetent in comparison, that adults will never be able to understand e-safety adequately.

Reality: *Adults tend to lead and children tend to follow. 'Facebook' started as an adult social networking site (and is still only officially available for those over the age of 13). It is true that children may be able to grasp technology quickly but it must not be forgotten that:*

- *children often lack maturity in understanding the dangers and consequences of their actions online*
- *children take risks as a normal part of growing up and this process now takes place online as well as offline*

It is vital that children are well supported as they explore the digital environment.

Myth: Online 'stranger danger' is not real
Reality: *Research has shown that in real life (as opposed to virtual), children are most at risk of sexual harm from people already known to them and that 'stranger danger' is less prevalent. However, in the context of the internet this is not the case, particularly when children are befriended online through social networking or gaming sites. A child may believe their new online friend is who they say they are when, in reality, they are an adult posing as a child (known at 'catfishing'). Most concerning is when initial online contact develops into face to face meetings.*

Myth: Online 'friends' are the same as real-life 'friends'
Reality*: In the online environment and social media platforms, the definition of a 'friend' has changed. Offline, we might consider a friend to be a person who is well known to us and someone we regard with liking, affection and loyalty, whom we have got to know through face to face contact. Over time, through regular digital engagement, people may consider themselves just as much friends with those they meet solely online, even though they may never have met in person, as those they regularly meet with face to face.*

Myth: Children don't engage with strangers on social networking sites
Reality: *When a young person is aware that their friends are part of a particular online community, they are likely to want to join in – whether it's sharing particular digital content, engaging with specific topics or communicating in a certain manner. However, as already mentioned, dangers can arise, especially when young people feel under pressure to engage with as many people online as possible or are not able to assess what is appropriate for them to share online.*

1.2.2 Internet safety for children and adults at risk

No matter how great the internet is for children and adults at risk to explore, there are some areas which are not appropriate for them.

Irrespective of which technology or digital space children or adults at risk use, they need to be aware of:

- Protecting their own safety.
- The risks involved in meeting people online and the danger of being groomed.
- The security of their digital footprints, which can lead to a loss of privacy, identity theft, data misuse and fraud.
- Cyber bullying, online fights, making threats and sexting.
- File-sharing, computer security and copyright law.
- Exposure to dangerous material such as pornography, racist and other hate-focussed materials, self-harm advocacy, drug paraphernalia, suicide and gambling.
- The addictive nature and dangers of overusing technology.

1.3 Potential problems online

1.3.1 Online grooming

Online grooming is when someone uses the internet to trick, force or pressure a child, young person or someone who is vulnerable into doing something sexual – like sending a naked video or image of themselves.

A person who is grooming others online will sometimes build their trust before talking about doing anything sexual. People can be exploited online without any physical contact ever taking place. The abuser, for example, could ask a child to send naked photos of themselves or perform sexual acts transmitted via a webcam.

Online grooming can be faster than grooming in person, due to the anonymity of the internet, resulting in children, in particular, trusting an online 'friend' more quickly than they would in a face to face encounter. People intent on grooming children online often use the same social media platforms which are popular with children and young people. Online grooming is a crime.

Abusers can use a range of techniques to make contact and establish relationships. These include:

- Gathering personal details online from social networking sites, multi-player games and other platforms.
- Offering opportunities for modelling, especially to young girls.
- Promising meetings with celebrities and offering gifts, such as computer games or tickets to concerts.
- Gaining the confidence by offering positive attention or providing a sympathetic response when personal problems are shared.
- Masquerading as a child or assuming another false identity in order to gain the trust
- Bullying, threatening or blackmailing.

Once the abuser has gained trust online, they might suggest meeting up in person.
There are a range of actions which can be taken by parents/carers and workers to prevent the risks of online grooming, including:

- Discuss the potential risks of online grooming with children and adults at risk. Do not wait for something to happen, but instead talk to them now, on a regular basis.
- Visit the National Crime Agency's Thinkuknow[1] website, which has a lot of useful information for parents, children's workers and children of various age groups.
- Highlight that the internet is a public place and that not everyone online is who they say they are.
- Use parental controls and safe-search facilities based on the age and maturity of children or adults at risk concerned. Remember, however, that these may not be 100% effective and are not a substitute for supervision.

1 www.thinkuknow.co.uk

- Explain that personal details should never be given out (e.g. Name, address, phone number, school, etc), and personal information should not be shared (including photos and videos) with strangers on any digital platform.
- Strongly encourage people to set their online social media profiles to 'private' so that only friends and family can see them.
- Set rules for the use of webcams, digital cameras and camera phones.
- Remember that people can be vulnerable to online grooming on all digital platforms, including multi-player gaming websites and social networking websites.
- Encourage people to talk about anything which makes them feel uncomfortable online (such as a stranger making contact), and to save emails, messages and any other evidence.
- Look for any unusual signs, such as children hiding their texts or messages, unknown adults contacting them or sending them gifts, or seeing dramatic changes in their behaviour.
- Report any incident of online grooming to the Child Exploitation and Online Protection centre (CEOP) as well as the police.
- Keep computers in an open room to allow effective supervision, but be aware that most children and adults at risk can access the internet on their phones without easy supervision.

If, as a worker, you are worried about the welfare of a child or adult at risk, you should follow the reporting procedures in ***Section 10: Responding to Safeguarding Concerns*** in Good Practice 5.

1.3.2 Digital footprints

Digital footprint is the term used to describe the virtual trail which people leave behind as they explore the internet. Every time someone does something as simple as visiting a website, information about the visit is stored on their computer and by the website itself. Anything which is posted on social media websites can be easily accessed by others and could remain there forever – even after you think it has been deleted.

Children and adults at risk often don't understand that what they do in the digital world could have huge implications to their reputation in real life over a long period of time, with anything posted online being searched for and retained by other people. Examples include:

- A blog or social networking profile containing comments, photos or videos a young person would not want parents, peers or teachers to see. It is not uncommon for university admissions tutors and employers to look up applicants online.
- Content and music downloaded and shared illegally, even unwittingly.
- Footage of an individual doing something silly, embarrassing or reckless being published and shared online.
- Intimate or naked photos shared with people via text or instant messaging (sometimes under pressure from their partner) which is passed around a wider group. This can make children and adults at risk, vulnerable to sexual exploitation.
- Nasty comments (often referred to as 'trolling' or cyber bullying) are made which they might regret later.

It is therefore essential that people are helped to understand the potential consequences of their behaviour in the digital world, so that they can protect their reputation in real life.

1.3.3 Digital reputations

It is important to help people think about the implications of posting images and comments online. Things to consider exploring with children and adults at risk:

- Encourage them to make the most of built-in privacy tools.
- Explain that every time they go online, they leave a trail.
- Encourage them, with supervision, to type their name into a search engine so they can see what comes up about them.
- Encourage them to ask permission before publishing any content involving their friends or family (and to ask their friends and family to do the same).
- Explain why it is important to be honest when registering for access to websites and services. Many social networking websites, video-sharing sites and blogs have a minimum age limit.
- Discuss with them the moral and legal issues surrounding the posting of material involving others (e.g. A negative comment about someone could be considered slanderous).
- Talk to them about the consequences of sharing intimate or naked images in the digital world, including through text messages (called 'sexting').

1.3.4 Misleading content

It is useful to explain to children and adults at risk that not all information on the internet is fact. Some of it might be deliberately misleading and/or designed primarily to sell commercial products. Social media Influencers are people with a large number of followers, who make a living from advertising products through their influence and ability to sell their perfect 'lifestyle'. It is not always easy to understand that they are selling products and not simply sharing their favourite brands and products.

Some websites will report 'fake news' or things that aren't completely true. They might do this in order to scare or to make people do something, such as visiting their website – because they make money from people going to their site. In order to spot fake news, check the name of the website and the web address to see if it looks real, and look at the reporting on known and trusted sites to see if they are also reporting it.

1.3.5 Identity Fraud and Phishing

Identity fraud or identity theft is the illegal act of using someone else's personal information without their permission, typically for economic gain.

Phishing is the fraudulent practice of sending emails pretending to be from reputable companies, in order to get individuals to reveal personal information, such as passwords and credit card numbers. It may not be immediately obvious that identity fraud or phishing is taking place, so it is essential to protect personal financial details at all times (including pin codes and passwords). Look out for the warning signs, too, such as debits on bank statements of which you are unaware.

Some useful tips include:

- Delete suspicious emails without opening them.
- Be aware that offers which seem too good to be true probably are.

- Install security software on all devices and keep it updated.
- Do not use the same password for all websites or services.
- Never respond to any unexpected email requests or callers looking for personal details.
- Do not respond to emails claiming to be from banks asking for personal details (banks never ask clients to submit this type of information by e-mail).
- Refraining from online purchases unless the URL begins with 'https://' and the padlock symbol is displayed beside it.

1.3.6 Cyber stalking

Cyber stalking is the use of electronic communications to stalk, harass or frightening someone. This may include making false accusations, defamation, threats, vandalism, solicitation for sex or gathering information in order to harass, embarrass or threaten.

1.3.7 Cyberbullying

Cyberbullying is no different from real life bullying, except that it happens in the digital world – someone being tormented, teased, threatened, harassed, humiliated or embarrassed. Cyberbullying may involve the use of images, text messages, phone calls and social networking profiles, and is just as unacceptable as bullying in real life. The only difference is that it is not restricted by time or physical location, and so it is therefore harder to escape from.

If someone believes they are being cyberbullied or cyberstalked, they should be encouraged to tell a trusted adult such as a parent, teacher or friend. Children should be aware of the Click CEOP button, present on some websites, through which abuse can be reported. Of course, it may also be necessary for the police to be involved.

1.3.8 Sexting

Sexting is the sending of sexually explicit photos, videos or messages. The content depicts someone in a state of nakedness or in sexually provocative or revealing positions. This indecent imagery, which is often self-generated, can be used to bully and blackmail, with the creator not fully understanding the consequences of what they have produced. Once made public, sexts are very difficult to retract and, apart from causing acute embarrassment and distress, such images can have far more serious consequences.

Sexting can occur in a number of scenarios, including:

- Partners exchanging images with each other (either with both partners' consent or with one partner under duress or without their knowledge).
- Partners sharing private images outside of their relationship, such as passing them around school. Ex-partners can be particularly vulnerable to this type of action, which is often referred to as 'revenge-porn'.
- Friends passing on sexting images which they have received.

Young people often start sexting 'for a laugh' but such behaviour could lead to serious consequences for everyone involved. In the digital world, images can be copied, manipulated or sent to other people within seconds – something which starts a private conversation between two people can quickly reach peers and even complete strangers.

Tips to help children understand the dangers of sexting, include:

- Talking to children about sexting, just as you would about any digital safety issue. This is especially important for older teenagers, who might be in a relationship.
- Discussing sexting as part of a wider conversation about relationships.
- Reminding children why it is important to think carefully before they post anything. It is very difficult to retract an image or piece of information once it is uploaded.
- Encouraging children not to pass on these kinds of images, even if they are being urged to do so by their peers.
- Explain that, under the sexual offences act 2003, it is illegal for anyone to take, hold or share indecent images of anyone under the age of 18 (even if they are also under the age of 18, and/or the content was created with the consent of that young person).

The police must, by law, record all sexting incidents on their crime system, however they can decide not to take further action against the young person if it is deemed not in the public interest. This is at the discretion of the police.

1.3.9 Exposure to inappropriate and harmful material

Another online risk is exposure to potentially harmful, user-generated content, including violent or pornographic images, gambling websites, self-harm websites or forums, radicalisation websites or forums etc. The content in question might not be illegal, but it could be upsetting, disturbing or otherwise generally unsuitable for children.

Children and adults at risk may come across unsuitable or upsetting content inadvertently, as well as actively looking for content, such as pornography, for example, out of curiosity.

What can workers do about inappropriate and harmful material?

Churches can help to avoid children and adults at risk accessing inappropriate and harmful material in the following ways:

- Children and adults at risk are supervised at all times when using church computers.
- Churches run regular sessions to help educate people about safe internet usage (the Synod Safeguarding Officer can offer advice).
- All people using church computers complete consent and behaviour forms, with expectations of use reinforced.
- Church computers and games consoles have appropriate age controls and safety features in operation.
- Filters on video-sharing websites are operational for church computers.
- The importance of age limits for websites and services are understood by children, as these exist to help protect them from unsuitable content.

1.3.10 Abusive/Illegal Images of Children

As the use of, and accessibility to, the internet has increased, so too has the production of abusive/illegal images of children.

The possession of abusive/illegal images is a form of child exploitation, despite it not necessarily involving direct interaction between the person possessing the images and the child. The terms

'abusive images of children' or 'illegal images of children' are preferred instead of 'child pornography', in order to highlight the seriousness of the offences. It is also important to be aware that pornography is legal (with some exceptions) yet the making, viewing or distributing of sexual images of children is never legal.

1.4 Advice and Support

1.4.1 Church websites

Here are some tips to help when creating, managing and editing your church website:

- Make sure websites are safe and appropriate for all users.
- When designing sites, make clear what is permissible to copy or use in other places.
- Obtain permission from parents, carers or children before using any pictures of children.
- Use group photographs of children, rather than individuals.
- Do not publish the name or location of any child.
- Do not publish personal email addresses, postal addresses or telephone numbers.
- Make web content as accessible as possible to people with disabilities e.g. using fonts which are easier for people with dyslexia to read.
- Appoint a responsible person to monitor the content of the website.
- Placing the CEOP 'report abuse' button on websites along with the link to the 'thinkuknow'[2] internet safety website. This offers effective and age appropriate advice for children, parents and carers.
- Complete a risk assessment before hosting message boards, forums or blogs and ensure that they are password protected.

Please note: Churches are responsible for all content contained within websites, blogs, social media or any other platforms maintained by them.

1.4.2 Use of Social Media Platforms

Social media platforms provide a range of opportunities for children and churches, such as:

- An attractive and powerful communications environment, albeit one in which children need close advice and guidance
- A strong sense of community
- A marketing tool for promoting the church and its various activities and groups
- An evangelistic platform

Social media platforms also carry a number of risks, including the facilitation of trolling, cyberbullying, cyberstalking and boundary drift when workers befriend children online. Direct messages via social media platforms should be avoided, but where they are used a record of the communication should be kept.

---

[2] www.thinkuknow.co.uk

Certain social media platforms have age restrictions and no URC worker should support a child accessing a platform they are too young for.

1.4.3 Workers befriending children online

If workers are to engage with children via social network sites, the advice from CEOP is that this should be done through a public page set up by the church, and not a personal social media account. The benefits of only interacting via a public church page are:

- Transparency.
- Ease of information sharing.
- Ease of management and administration by an individual or team.
- Providing an area for children to interact with each other safely, with supervision and no obligation to interact via their own personal pages.
- Clear boundaries for the worker, and a maintained level of privacy.
- Reduced risk of personal information being used against the worker e.g. bullying.
- Reduced risk of accusations of professional misconduct as boundaries are clearly maintained.
- It is easy to monitor what is being said to a child when communication is all via a public platform.

1.4.4 Filming and photography

Organisations should take great care in the ways in which they create and use photographs or film footage involving children. This does not mean that pictures or filming should be prohibited, but in order to safeguard children it is recommended that the following steps are taken:

- Permission should be obtained from parents/carers before a photograph is taken or film footage recorded.
- Parents/carers should be asked NOT to take photographs that include any child who is not their responsibility, unless permission has been granted.
- It must be made clear why images or films are being made, what they will be used for, who might see them and where they will be stored.
- Children and young people should be asked if they want to be filmed or photographed.
- Use group photographs of children where possible and ensure that individuals cannot be identified by any personal details such as their name, school badge, age or address.
- All photographs should be appropriate and respectful of the subject.
- Photos and other digital media should be stored in a secure location, ideally on a church computer. If this is not possible it is important to record where the photographs and digital media are stored.
- Consent forms should contain a section covering consent for photography and digital media. See Appendix F: Sample Information and Consent Form.

1.4.5 Electronic communication with children and young people

When communicating with children and young people via email, messaging and other forms of electronic communication, it is advised that:

- where possible, communication is via parents rather than directly with children
- parental consent is obtained for electronic communication with children – making it clear what type of communication will be used (e.g. Text messaging, email, social media platforms etc).
- digital communication does not take place with children under the age of 13.
- standardised group communications are used where possible (e.g. group emails and WhatsApp group messages etc).
- communications are transparent and a record is kept of anything which is not visible to others online.
- communications are not at anti-social hours.

1.4.6 Technology Addiction

Children and young people can spend many hours on digital platforms. To help avoid excessive use of technology, clear boundaries are needed for children when using digital platforms. This might include the length of time they are allowed to spend on computers, the kind of websites they can visit, which games they are permitted play, limiting the amount of data they can download to their mobile phone, etc.

1.4.7 E-Safety, acceptable use policy & safeguarding policy

Within the Safeguarding Policy of Staplehurst United Reformed Church there is a section on e-safety, including the expectations of workers in their electronic communications with children. It includes an acceptable use policy in relation to the use of church computers by both workers and children. This includes sample forms which children and workers will be asked to sign.