Contents

1. E-safety Definition

E-safety, or electronic safety is the collective term for safeguarding involving the use of mobile phones, computers (laptops, tablets) and other electronic devices including games consoles, to communicate and access the Internet, emails, texts messages, social networking sites and other social media.

The technology is constantly advancing bringing with it additional safeguarding considerations. This e- safety policy reflects all communications between workers and children/young people (those under 18 years of age) recognizing that online and offline worlds are merging as well as the distinctiveness and difficulties within faith based organizations of defining clear boundaries for everyone.

This e-safety policy includes guidance on both fixed and mobile internet technologies. e.g. PCs, laptops, tablets, web cams, digital video equipment, mobile phones, digital cameras and portable media players and any other forms of mobile communication device being used.

2. Kairos Network Church's Commitment to E-safety

We will exercise our right to monitor computer systems being used for the purposes of any church work and during any church activity. This will include access to websites, the interception of e-mail and the deletion of inappropriate material where it believes unauthorized use of the computer system is or may be taking place; or the system is or may be being used for a criminal purpose or for storing unauthorized or unlawful text, images or sound.

When using a computer or electronic device with internet at the church children will not be permitted to:

- Search for and/or enter pornographic, racist or hate-motivated websites;
- Download, forward-on, copy or burn onto CD any music, images or movies where permission has not been granted by the copyright holders;
- Disclose any personal information e.g. addresses (postal, email or social media), phone numbers, bank details. This includes personal information about another person;
- Send or display offensive messages or pictures;
- Use obscene language;
- Violate copyright laws;
- Trespass in others' folders, work or files (i.e. enter without permission);
- Retrieve, send, copy or display offensive messages or pictures;
- Harass, insult, bully or attack others;
- Damage computers, computer systems or computer networks;
- Use another user's password;
- Use computers for unapproved commercial purposes.

Sanctions:

- Violations of the above rules will result in a temporary or permanent ban on Internet use.
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
- When applicable, police or local authorities may be informed.

3. Children and Young People will be expected to make appropriate and safe use of internet technology

Safe internet use will be included in our children and youth ministry programs at the start of every academic year and as needed.

Every child or young person who is communicating online as part of any church activities will be required to agree to the following expectations for responsible internet use. These are also written into the Kairos Network Church's Code of Conduct for Online Communication:

- I will not share passwords or usernames with anyone.
- I understand that I must not bring software into the church without permission
- I am responsible for any messages that I send and for contacts made. I will only send messages which are polite, sensible and free from unsuitable language.
- I will not send any attachments which are hurtful, abusive or offensive. This also applies to chatrooms on video conferencing.
- If I receive anything, see anything or come across a website which may be unsuitable or makes me feel uncomfortable I will immediately tell a responsible person [Emma James] and/or the church safeguarding officer.
- I understand that I must never give my home address, phone number, send photos, give out personal information, or arrange to meet someone who contacts me over the internet.
- I will not send anonymous messages.
- I understand that if I deliberately break these rules my parents/guardians will be informed.
- I am aware that the church has a Code of Conduct for online use and I have signed it.

Rationale:

Responsible internet use will be included on the general consent form the parent/guardian signs before a child or young person joins any group, club or activity. Parents / guardians will also be made aware that the church's e-safety policy is available on the church website.

If the parent/guardian requests their child is not communicated with via online technology, this must be respected and an alternative found.

It is the joint responsibility of workers, the church and the parent or guardian of the child to educate them about their responsibility when using the Internet.

The above expectations are written into the church Code of Conduct for Online Communication and should be signed by the child and their parent/guardian.

Ensure all messages can be viewed if necessary by the young people's worker and safeguarding officer. Although unlikely to happen, this can help deter bullying and insulting or abusive messages.

4. We will make appropriate use of any Photographic and/or Video Images taken during church activities

Clear guidelines must be operated when taking photographic and video images of children and young people involved in church activities as follows:

- Permission will be sought before any images are taken and/or displayed. Images should only be used in the way and for the specific purpose agreed by the person photographed or if under 18, their parent/guardian.
- Written consent must specify what purposes the image will be used for, and how it will be stored if not destroyed.
- Photographs that include children or young people will be selected carefully and will not enable individual children to be identified by personal details. These details include e-mail or postal address, or telephone numbers.
- Children's full names will not be used by Kairos Network Church anywhere online in association with photographs which would make the child identifiable.
- Further written consent is required if images are to be used in other ways than originally specified.
- Ensure that any use of images reflects the diversity of age, ethnicity and gender of the activity.

Rationale:

Parents will be given the opportunity to decide if they want pictures of their son/daughter to appear online via a consent form.

A list of parents who do not require their son/daughter to appear online should be kept and regularly updated. This ensures that privacy is respected and no embarrassment is caused.

The policy should apply to all images and audio content be it still photographs, films or audio clips. Images count as personal data under the Data Protection Act 2018.

5. We will respond appropriately and sensitively to all e-safety concerns.

If an e-safety incident occurs, this will be reported to Kairos Network Church's designated safeguarding officer in the same manner as the reporting of any other safeguarding concern. They can then determine if the matter should be reported to the statutory authorities or other appropriate agencies e.g. Diocese of Leeds safe-guarding advisors.

Rationale:

The Kairos Network Church's Safeguarding Policy will be followed.

6. We will make use of appropriate confidentiality.

All children and young people have the right to confidentiality unless abuse/harm is suspected or disclosed.

Rationale:

Children and young people may find it easier to communicate online as nobody is physically present. This means the child may be more willing to share personal and sensitive information about themselves or a given situation than they would face to face.

Whilst it is entirely appropriate to offer general advice and support, ensure that the worker points the child or young person towards professional counselling if necessary.

7. We will make appropriate use of mobile phones where they are needed.

Use of mobile phones will be guided by the following considerations:

- ○ Any online communication between church workers and children will only take place after parental permission has been given. Once permission is given, staff and volunteers can hold mobile phone numbers of the children in their care.
- ○ Where appropriate, group messaging rather than individual messaging will be used.
- ○ Take care with the language and content used, avoiding ambiguous abbreviations such as 'lol' which could mean 'laugh out loud' or 'lots of love'.
- ○ Any messages or conversations that raise concerns should be saved and passed on/shown to the safeguarding officer.
- ○ Workers should not keep images of children on their mobile phone. Any images of children taken on a mobile phone should be downloaded to a church computer, stored securely and deleted from the worker's phone.
- ○ The church recognizes that personal mobile phone numbers do need to be given to children / young people but only with the agreement of the parents and leaders. This will be done via a consent form.
- ○ Workers should not make contact with young people after 9.30pm at night or before 7.30am in the morning, unless in exceptional circumstances or off-site together.
- ○ Workers should enable a password/lock on their phone for data protection and do not allow unauthorised access.

Rationale:

It is advisable that the young people's worker be supplied with a work-dedicated phone. This way, all calls and messages can be accounted for. It also protects the worker's right to a personal life outside work.

Workers and volunteers should ensure that they only take photos of children and young people in accordance with the guidelines above.

Workers and volunteers should recognise that messaging is rarely an appropriate response to a young person in a crisis situation or at risk of harm.

8. We will make safe and appropriate use of social networking sites when communicating with young people.

When using social networking sites, we will ensure that the following guidance is used by all workers:

○ Communication will not take place between the hours of 9.30 pm and 7.30 am, unless in exceptional circumstances or off-site together.

○ Parents /guardians will be informed of the minimum age requirements for different social media sites (eg 13 for Facebook and 16 for WhatsApp.) and will be asked to give consent before any communication takes place.

○ Any social media group set up by Kairos Network Church will always be closely monitored by the young people's worker and safeguarding lead.

○ Children/young people should be made aware that conversations may be recorded and kept (via text files or similar).

○ When using social media, workers and volunteers should contact children and young people through the social media account that is set up for the children / young people of Kairos Network Church. This should be done in preference to adding young people to their personal accounts.

○ Workers should seek to ensure that their personal profiles on any social networking sites are set to the highest form of security to avoid young people accessing personal information or seeing any pictures of a personal nature.

○ Messages sent to young people regarding youth activities should be posted openly and 'inbox' messaging should be avoided. If this is necessary in exceptional circumstances, a copy should be kept.

Rationale:

The same protocols for workers communicating with children and young people via mobile phone should apply to social media use. In other words, care needs to be taken with regard to language and content as well as when and for how long a communication lasts.

Use of social networking sites by workers makes it harder to boundary their private life, and also opens up the possibility of relationships between 'friends' who are children and 'friends' who are from the workers' adult personal world.

There are risks both for children and also for workers, who may find images and text appearing on their profiles which can be damaging to their reputations and positions as role models.

9. We will make safe and appropriate use of video conferencing media

When using video conferencing apps, we will ensure the following guidelines are used:

○ Use of web cameras and any video conferencing apps such as Zoom must only be used after parental permission has been granted. Best practice would be to avoid using such methods on a one to one basis, however, the church recognises that at certain times, this may be necessary.

○ Use a new meeting room each time. (ie don't use the your personal meeting ID)

○ A waiting room should be set up by the host and in this way, attendees are unable to join before the host. Two leaders must be available to attend every online meeting

- Young People will be advised not to undertake video calls in their bedrooms. If this is the only room available to them, they should change their background so that their bedroom remains private.
- The attendees will be muted on joining.
- Always lock the meeting room after the meeting has started.
- The meeting link should not be posted on social media and neither should the screenshot be shared if the meeting ID is visible.
- Best practice is to have two leaders on each call and to designate someone whose job it is to 'manage the room,' and focus just on this.
- If the meeting is aborted due to technical difficulties, a new link will be sent by another leader.

Rationale:

Following the above guidelines will ensure that all involved in video conferencing are kept safe.
The same protocols for workers communicating with children and young people via messages and mobile phone should apply to video conferencing. In other words, care needs to be taken with regard to language and content as well as when and for how long a communication lasts.