Appendix C

The United Reformed Church

Model church online safety policy

Church .....

Synod .....

(policy last updated: January 2019)

This is a model local church online safety policy, which should be used as a starting point to help your church put your own policy in place. It is important to note that this is not a 'catch-all' policy. It covers the broad basics of good practice, but it will need to be adapted depending on the individual circumstances of your church. It is also important to remember that an online safety policy alone is worthless without proper implementation and a church-wide commitment to the policy. We hope that you will find this sample policy useful. If you have any questions about policy, or safeguarding generally, please contact your Synod Safeguarding Officer for support and guidance.

Sample Online Safety Policy – January 2019

Published by the United Reformed Church communications office
on behalf of the Safeguarding Office.

Designed by Church House graphics office
Printed in Church House, The United Reformed Church,
86 Tavistock Place, London WC1H 9RT

The United Reformed Church

Introduction

Technology is constantly advancing, bringing with it additional safeguarding considerations. An online safety policy is necessary to safeguard all electronic communications between the church and children/young people (those under 18 years of age) recognising the merging between online and offline worlds and the distinctiveness and difficulties within faith based organisations of defining clear boundaries for everyone.

This online safety policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of online technologies for adults and children within this church, including the use of mobile phones, computers and other electronic devices.

It explains what will happen in the event of unacceptable use of these technologies and details the support that will be provided to support children, parents and others in the safe and responsible use of these technologies beyond the church.

Why we have a policy

The use of the Internet and mobile devices has become an integral part of church and home life. There are always going to be risks to using any form of communication which lies within the public domain. It is therefore imperative that there are clear rules, procedures and guidelines to minimise these risks and especially when children use these technologies.

It is also important that workers and church members are clear about appropriate procedures so that they are safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

This church acknowledges that whilst we will endeavour to safeguard against all risks we may not be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to policy to ensure that children are best protected

Policy Aims

- to ensure the safeguarding of children within and beyond church by raising awareness of appropriate and acceptable uses of online technologies
- to outline the roles and responsibilities of everyone involved
- to have clarity about procedures following the misuse of any online technologies
- to work with parents / carers and to maintain a continued awareness of both the benefits and potential issues of online technologies

Our commitment to online safety

We will equip children with the skills and knowledge that they need to use the technology in this church safely and responsibly, and to manage the possible risks. We will also ensure that they are aware of where they can go to get help, apart from trusted adults, if they are uncomfortable with anything in the digital world.

Children and Young People are expected to make appropriate and safe use of the electronic communication (devices)

When using a computer or electronic device with internet access at this church, children will be made aware of what is acceptable usage and will agree not to:

- search for and/or enter pornographic, violent, racist or hate-motivated websites
- download, forward-on, copy or burn onto CD any music, images or movies from the Internet where permission has not been granted by the copyright holders
- disclose any personal information eg addresses (postal, email or messenger), telephone numbers, bank details, including personal information about another person
- send or display offensive messages or pictures
- deliberately browse, download, upload or forward material that could be considered offensive or illegal
- use obscene language
- violate copyright laws
- trespass in folders, work or files belonging to others
- 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
- further action may be taken such as informing parents / carers
- when applicable, police or local authorities may be informed

Appendix C1 has an example of expectations that children/young people and/or parents/carers could be asked to sign.

We will make appropriate use of any photographic images and/or video footage taken during church activities.

Clear guidelines will be operated as follows:

- permission will be sought from parents / carers before any images are taken and/or displayed. Images will only be used for the specific purpose agreed by the person photographed
- written consent will specify what purposes the image will be used for, and how it will be stored. For instance if the intention is to use an image on the church website or other forms of publicity, this will be clearly stated at the time that consent is sought
- further written consent will be sought if images are to be used in ways other than originally specified
- if children object, even if parents / carers have agreed, their wishes will be respected
- photographs that include children will be selected carefully and will not enable individual children to be clearly identified

- children's full names and/or other details will not be used anywhere in association with photographs or other media
- when using photographs of children, group pictures will be used wherever possible
- any use of images will reflect the diversity of age, ethnicity and gender of the activity
- personal mobiles will not be used to take photographs or other digital media
- except in exceptional cases, which will be agreed, and known about, digital media relating to children will be stored on church computers. Should this not be possible for any reason, where the media is to be stored will be recorded

We will ensure that appropriate safeguards are in place, including the use of filtering software on all computers used within this church.

To ensure that unwanted and unsolicited information, viruses and other malware does not intrude on the use of digital technology, we will ensure all appropriate and reasonable steps are taken to protect computers and the users of them as follows:

- filtering software will be installed on all computers used at this church or as part of any activities operated by the church.
- on our church website/s, details will be prominently displayed as to where to find help online including having the CEOP button on the website

We will respond appropriately and sensitively to all online safety concerns.

In the event of concern that there may be an online safety incident, this will be reported to the church's designated safeguarding co-ordinator in the same manner as the reporting of any other safeguarding concern. The safeguarding co-ordinator will then determine if the matter should be reported to the statutory authorities or other appropriate agencies, including CEOP or the Internet Watch Foundation. In case of church's designated safeguarding co-ordinator not being available, the matter needs to be reported to the synod safeguarding officer.

We will operate safe email communications with children and young people.

When using email to communicate with children and young people, workers will:

- obtain parental agreement before they use email services to communicate with a child or young person
- use clear, unambiguous language to reduce the risk of misinterpretation
- ensure that all messages can be viewed if necessary by the worker's supervisor and that this policy is explained to children and young people.

We will make appropriate use of mobile phones where they are needed.
Not every child or young person has the use of a mobile phone and, even if they do, parents may not want a worker to have the number. Workers will therefore have alternative means of communication and will ensure that communication goes through parents if this is their preference.

Mobile phones should only be used where necessary and will be guided by the following considerations:

- where appropriate group rather than individual texting will be used
- care will be taken with the language used, avoiding ambiguous abbreviations such as 'lol' which could mean 'laugh out loud' or 'lots of love' and always end with people's name.

- any texts or conversations that raise concerns will be saved and passed on/shown to the worker's supervisor
- any images of children taken on a mobile phone will be downloaded to the church computer and kept securely
- workers will not take or keep images of children on their personal mobile phone.
- workers will not give out their personal mobile number to children
- as well as ensuring that calls / texts are not sent after 9pm or before 9am, workers will also ensure that calls and texts are not sent whilst the child is at school / college, as this may be against the educational establishment's rules
- workers will enable a password/lock on all devices to ensure data protection and will prevent unauthorised access being gained

We will consider the appropriate use of Chat & Messenger Services and whether these are necessary.

Instant Messenger Services (IM) are internet programmes that allow people to write and receive messages in real time.

As with other forms of online communication, workers will take care with regard to language and content, as well as when and for how long a communication lasts.

Workers will ensure that all communications using IM services adhere to the following:

- communication will not take place between the hours of 9 pm and 9 am *[or alternatives]*
- workers will ensure that they enable settings when using IM services which allow for significant conversations to be saved as text files and will keep a log of when and with whom they communicated
- children/young people will be made aware that conversations will be recorded and kept (via text files or similar)

We will make safe and appropriate use of social media platforms when communicating with young people.

When using social media platforms we will ensure that the following guidance is used by all workers:

- workers will not add young people with whom they work to their personal social media platforms if they are under the age of 18.
- workers will set up a Facebook group / page for the church or church group and invite young people (in the appropriate age group) to be members
- workers will only use an agreed social networking account for contact with young people with whom they are working
- workers will to ensure that their personal profiles on any social media platforms 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 will be posted openly and 'inbox' messaging should be avoided. If this is necessary in exceptional circumstances, a copy will be sent to an identified person to assist transparency

Sanctions

Workers will be made aware that not complying with any of the above will incur sanctions, which could include suspension or dismissal and referral to appropriate authorities.

Appendix C2 has an example of an Acceptable Use Policy that workers could be asked to sign.

We will store data securely

There are a variety of ways that data can be stored. Where data of any form about children is stored this will be password protected and in general be stored securely on the church premises. If this is not possible then a record will be made of where the data is stored. Where it is necessary for data to be transported, memory sticks will be purchased for workers so that there is a separation between personal and church information.

Appendix C1
Child Agreement

Children and young people agree to the following expectations for responsible use of technology:

- Where using a social media platform I will use only use my own login and password which will be kept secret
- I will not deliberately browse, download or forward material that could be considered to be offensive or illegal, for instance pornographic, violent, racist or hate-motivated material
- I understand that I must not bring software into the church/organisation without permission
- I understand that I must not violate copyright laws
- I am responsible for email that I send and for contacts I make. I will only send messages which are polite, appropriate and free from unsuitable language.
- I will not send any attachments which are hurtful, abusive or offensive
- 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 [name/title of worker], or report it to The Child Exploitation and Online Protection Centre (CEOP) or the Internet Watch Foundation
- 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 and I know that chain letters are not permitted.
- I understand that any youth and children's workers (add if others) are not allowed to accept friend requests via social media platforms
- I understand that if I deliberately break these rules, I will not be allowed to use the Internet at church and that my parents / carers will be informed

Signed .....

Name [Print] .....

Dated .....

Appendix C2
Worker Agreement

To ensure that all adults are aware of their responsibilities when using any online technologies they are asked to sign their agreement to specific Acceptable Use Rules. This is both to provide an example to children regarding safe and responsible use and as a safeguard from any potential allegations or inadvertent personal misuse.

These rules apply to all online usage and to anything that may be downloaded or printed.

General:

- I have been given a copy of the church online safety policy to refer to for all online safety procedures I should follow
- I know who the church Safeguarding Co-ordinator is
- I will only use church equipment in an appropriate manner and for professional uses (nb if portable equipment is taken home I will ensure my home insurance covers this)
- I will adhere to copyright and intellectual property rights
- I will take measures or seek advice to prevent the introduction of viruses to the network.
- I will ensure that all devices, including memory sticks, containing information about children are password protected and that I keep my password secure
- I will report any accidental misuse
- I will report any incidents of concern to the church Safeguarding Co-ordinator

Photographs & video:

I know that:

- all images should be appropriate and beyond first names not reveal any personal information about children if uploaded to the Internet. Images should only be uploaded with permission from the parent / carer, as well as the child involved
- I should not take images on any personal devices. If in exceptional circumstances such use is felt necessary it should be agreed in advance or reported promptly to the church Safeguarding Coordinator
- Images of children should be stored securely on the church computer, never on personal devices, including memory sticks

Communication & Social Networking:

- I will ensure all messages are written carefully and politely
- I will not keep communications secret from those in the church to whom I am accountable
- I will not communicate with children online without consent from a parent / carer

- I realise that I am putting myself at risk of misinterpretation and allegation should I contact children via any systems other than those agreed
- I will not accept or request the 'friendship' of children/young people via social media platforms
- I understand the value of setting my 'Privacy' settings appropriately on any social networking site
- I will keep a record of any online communication with a child
- I will not publish, post or release information that is considered confidential by the church, a young person or anyone else

I have read, understood and agree with the online safety policy and the rules specified above and understand my responsibilities regarding safeguarding children when using online technologies.

I also understand that if I fail to follow agreed procedure there will be sanctions that could lead to my being suspended or dismissed, once appropriate procedures have been followed.

Signed .....

Dated .....