1.3L GUIDANCE ON SOCIAL AND DIGITAL MEDIA

In all their contacts and communications with the children of their group, all church personnel must be open and transparent in their digital communication with children, as in all other forms of communication.

Church personnel should not communicate with children using their personal social media accounts or personal email.

For a group/Parish using/publishing a social networking site a thorough Local Safeguarding Risk Assessment should be undertaken ***(Guidance 1.3A)***. The following guidelines should be considered as part of this.

- An Acceptable Usage Policy should be devised when publishing a social networking site or using church I.T. equipment.
- Be aware that different platforms have different restrictions in relation to age. Church personnel must ensure compliance with age restrictions within the terms and conditions of use of your chosen platform.
- Avoid the use of social media platforms that share contact details with all users. Church personnel may inadvertently connect young people up with other people as an unintended consequence.
- There are a range of video conferencing platforms available. When using these platforms, ensure you use the most up-to-date guidance for security. For applications which allow for password access, only use password/passcode protected meetings, create a new password for every meeting, and send details securely to participants (do not, for example, share details on social media). The password should be held by at least two people. Passwords should only be sent to parents/carers of children and young people and not directly to the child/young person. Enable the 'waiting room' feature, where available, which allows the host to have the discretion to allow invitees in to attend the meeting.
- Use of social media is beyond the normal running of your group and therefore needs clear permission before use in the following ways:
  - You must have Select Vestry/Parish Panel approval – speak to your Rector, Parish Panel or Select Vestry to discuss and minute that this is happening. Why not trial a video conference with some of these people first? This does not need to be a complicated process.
  - You need parental consent – set up an email which explains what you are doing, the date and time of the video conference session, which youth leaders are participating and what you roughly will be doing. We advise these conference calls not to take place after 9:00pm at night. Ask for a reply as a form of consent and keep these emails in a separate folder.
  - Use parents'/carers' email addresses to send the meeting invite to as this ensures parents/carers are aware that it is happening and can set up the young people to access the session appropriately with any oversight if they want.
  - For children under 11 a parent/carer must be in the room when they are taking part in an activity online.

- 'Normal' youth group rules would apply, including with regards to recruitment and safeguarding process – i.e. you need at least two safely recruited youth leaders present who would normally have 'real time' contact with this group. Make sure both leaders are live before young people arrive. Ideally use the same time slot as your normal youth group meeting.
- Codes of Behaviour for church personnel should be followed as you would expect in the usual youth group setting.
- As always, be inclusive – are there any young people from your group who would struggle to participate in this way, and what extra support can be put in place for them?
- As well as the video interface, there is usually space to write comments and participants can screen share too. Consider use of this facility and whether to disable it, or ensure it is appropriately monitored and controlled.
- Be aware of and sensitive to technical difficulties! There can be issues with speakers and microphones! Chances are young people will have this sussed, but leaders may have issues. Use the software with leaders first to try and sort out any difficulties in advance of the meeting.
- DO NOT RECORD. Most video conferencing software allows for the session to be recorded – this is an option for the host of the meeting only. Avoid doing this, as you would need separate permission for data capture and there are all sorts of issues around storage, data protection, etc.
- The site should be monitored by a designated supervisor.
- Any inappropriate posts should be removed by the designated supervisor immediately after it comes to their attention. Where possible, sites should be monitored before content is put up.
- The site should be kept 'private' or 'closed', i.e. only permitted members or 'friends' can see what is posted on the site.
- The use of personal addresses and telephone numbers, etc., should not be used even if sites are 'private' or 'closed', as there is the potential for items to be copied and shared.
- Content of any postings should be consistent with the aims of the Parish/ group. If in doubt church personnel should seek advice from the Parish Panel.

Church personnel using a social media apps for church activities or to communicate with young people:

- Parents/carers should be asked to give their consent for church personnel to communicate with their child via email, social/digital media (1.3K Template 1). For those parents/carers who wish to become members of any church-related social networking site group they should be asked beforehand to ensure that their own privacy settings are suitable and reminded that they should not accept any friend request from a child from the social networking site group other than their own. They should also be informed that their participation in such a social network group is subject to these standards.

- Should not 'Friend' or 'Follow' children on social media (unless a familial relationship exists). It is possible that children will seek to 'Follow' church personnel on social media, so church personnel should make sure any content they post is appropriate or ensure their privacy settings are set appropriately so that children cannot access the content.
- Messages left to or from children on social network sites should be written on an open page and not in a private message, or by using 'chat' [one-on-one].
- Should not network with members of their group via closed [one-on-one] communication, e.g. Facebook Messenger, WhatsApp, etc. Networking should be done through 'Group Chats' with a minimum of two adults in the group chat as administrators.
- Any events or activities run by the group/Parish that are organised or publicised on the site should be a closed event so that non-members cannot access the event without suitable permission by the site administrators.
- Church personnel should be cautious sending emails directly to children. Any emails sent should also be sent to at least one other church person and should be done with the consent of the child's parent/carer. BCC should be used when sending group emails to avoid sharing other children's email addresses.
- Should avoid communicating with children in their organisation/group via social/digital media late at night or during school hours.
- In signing off a post or an email, church personnel should not do so in a way that could be misconstrued or misinterpreted by the recipient. Simply sign your name.
- Any disclosures of abuse reported through a social networking site must be dealt with according to the reporting procedures ***(Guidance 2.1A).***

1.3L TEMPLATE 1: CONSENT FORM FOR SOCIAL MEDIA

Insert name of group:

SOCIAL/DIGITAL MEDIA CONSENT FORM

The clergy, staff and volunteers of the above group wish to use social/digital media to contact your son/daughter (aged 13 years plus) to inform him/her about the ongoing activities and special events of the group.

CONSENT

Name of Child:

I give permission for

Insert name of group:

to contact my son/daughter directly via the following methods:

Please tick the boxes below to give permission for the particular item.

Text messages

E-mails

Insert social networking site:

Contact Details (of child) - fill in if applicable

Mobile:

Email:

Signed parent/carer:

Date:

(This consent may be incorporated into the Sample Consent Form 1.3C Template 1).

In line with Data Protection regulations, we are committed to protecting the personal information given on this form. By providing the information requested, you are giving us permission (consent) to use this information for Safeguarding, legal or regulatory purposes and we will use it for no other purpose without further consent unless mandated or required to do so under the Data Protection Act 2018 or equivalent legislation. If you have any questions about how we process your personal data, please contact a member of the Parish Panel.