

Dear Parish Volunteer,

## **Re. Updated Safeguarding guidelines for online communication and video conferencing.**

The unprecedented times we are living through have led many of us to find new and creative ways to meet with people from our parish communities.

Whilst having to adjust to the situation, it is important that we continue to follow safeguarding procedures to ensure the safety and protection of all, but in particular those who are vulnerable or at risk. Everyone in the Church has a responsibility to safeguard and promote the wellbeing of those who worship in our Church or who join us for any activity facilitated by Church members.

Online platforms and new technologies offer tremendous opportunities to reach, communicate, evangelize, and engage with those involved in the Catholic Church. The use of technology and social media platforms has the potential to transform the way in which we can communicate and continue with some forms of ministry at this difficult time. Keeping everyone safe whilst using these platforms is essential, and as it is a new experience for many, it is important to understand how to implement some simple steps that can contribute towards keeping people safe online.

To remind you, the use of online platforms to meet socially or to livestream events, carries a particular risk when young or vulnerable people are taking part. The following guidance has been recommended for the protection of yourself and young people/vulnerable adults.

- **What is the purpose of the meeting?**
  - If it is to share information which is relevant to the whole group, could this be done through your existing communication channels for which you already have sought parents/carers consent?
  - Could the information be shared on the parish website?
  - Could a video be pre-recorded and shared via the parish website?
- **The Parish Priest and the Parish Safeguarding Rep should be notified of the online meeting.**
- **Organisers of the meeting must have been safely recruited by the Diocese.**
  - For more information, please contact Nathan Keogh:  
[Safeguarding@diocesofsalford.org.uk](mailto:Safeguarding@diocesofsalford.org.uk)

### **General Principles**

- It is not appropriate to use personal social media accounts, phone numbers or email addresses to contact participants, without the consent of those legally able to give it.
- Respond to concerns immediately.
- Always use age-appropriate language in your communications and make sure all your communications are relevant to the work of the project you are involved in.
- Understand how different social media platforms work and what their age limits are – for example you should never use Facebook to communicate with under 13 year-olds. Use NetAware to find out about age restrictions on social networks, apps and games.

- There is an NSPCC podcast for more tips on communicating with young people online – make sure other volunteers have listened to it – take a record who has undertaken this training.
- When setting up online youth groups, can you please notify the diocesan youth office at: [youth@dioceseofsalford.org.uk](mailto:youth@dioceseofsalford.org.uk).

### **Communication and Online Platforms**

- Once the platform is selected, it is advisable to set up a custom account in the name of that group, parish or body, accessible to more than one person who can act as ‘administrator’, using a strong password (Minimum of two moderators).
- Ensure that the administrator/host is aware of the settings that will maximise security and that they are confident and competent in using them. (Please ensure the moderators have completed the educare safeguarding module and the online safety module (<https://www.educare.co.uk/>).
- Communication should always be via parish email account. A generic email address or telephone number associated with the group, accessible to more than one person who can act as administrator should be used in order to maintain appropriate boundaries. The benefits of this are that:
  - communications can be easily reviewed by other leaders or helpers in the event of enquiries;
  - the need for action on any matter can be easily shared and delegated;
  - communications can be picked up in the event of sickness or other absence;
  - all correspondence and data is stored securely in one place.

### **Setting up an online meeting:**

- Set up a registration system to log the details of those who want to attend so that they can be sent a private message, securely by email or other closed group correspondence, with a randomly generated link and the password. Ensure that this is copied to parents and carers as well;
- If using meeting ID’s instead of links to host public events, use the randomly generated ID at the time of scheduling the meeting, rather than a personal meeting ID which is given when an account with the chosen platforms created.
- Ensure that joining instructions provide information on the ‘rules of engagement’ include:
  - when and how participants can speak/contribute;
  - how they should present themselves on screen (ie dressed appropriately, backgrounds);
  - how to interact with others;
  - how and when participants can leave the meeting;
  - what to do in respect of re-joining if internet connections fail;
  - that communication must be respectful and individuals must take personal responsibility to ensure that their content is appropriate to those participating e.g. language, jokes, opinions;
  - how to report anything of concern or anything that makes them feel uncomfortable.

- Obtain in advance any agreement to audio or visual recording of the meeting <https://www.dioceseofsalford.org.uk/youth/resources-links/consent-form-for-use-in-videoconferencing/>. For children or individuals who lack capacity, consent must be obtained from the person legally able to provide this. Those giving consent must be informed of the purpose the recording will be used for and for how long it will be retained. If images are being captured, this must be in line with GDPR (2016)<sup>1</sup>;
- If material is going to be used for a different purpose than the original intention, the new purpose must be explained and consent obtained.

### **Conducting an online meeting**

- Set up a ‘waiting room’ so that the meeting host chooses when to admit people and can restrict entry to only those who are invited;
- Lock the meeting once it has started;
- Where possible appear before a neutral background;
- Remind participants of the agreed rules of engagement;
- Mute attendees and ask them to hold their hand up if they want to speak so the host can unmute them;
- Keep sharing screens restricted to the host and limit chat to the host only if necessary to avoid separate conversations taking place during the session;
- If consent has been given to share screens shots during the meeting, ensure that the participants ID is not visible to an external audience;
- Do not post or request personal information that is unrelated to the purpose of the meeting e.g. private email addresses, birthday, phone numbers;
- Never accept or open files, or reply to any instant messages or contacts, phone calls, video call or screen-sharing request from someone that is not known or was not invited the online meeting;
- Ensure any incident involving inappropriate behaviour is recorded and responded to in line with policies and procedures;
- When meetings close, the platform should be closed to all. Nobody, other than the meeting facilitators should be asked to remain on-line for a one-to-one conversation without others being present.

### **Parental/Carers Consent:**

- Has permission been sought from parents/carers to communicate with the young people using this platform? These can be assessed via the diocesan website: <https://www.dioceseofsalford.org.uk/youth/resources-links/consent-form-for-use-in-videoconferencing/>

---

<sup>1</sup> Whenever a person’s image is captured, be it by camera, video, web camera, mobile phone, or CCTV, and that person can be identified, the image is likely to be considered personal data. This means that the image must be processed in line with the data protection principles. Processing means anything that is done to the image for example recording it, using it or sharing it. For the Church to use images of people that enable those people to be identified, they need a lawful basis

- Clear information should be provided to parents and carers about the purpose of any online activity, the range of people participating e.g. children, adults, mixed, and the names and contact details of those responsible for the activity.
- Parents and carers should be encouraged to ensure that participation takes place in a place visible to others within the household and not within bedrooms or other closed spaces.
- Parents and Carers should be encouraged to ensure there are parental controls on all devices [you can find out more about this on the NSPCC website <https://www.nspcc.org.uk/keeping-children-safe/online-safety/parental-controls/> ]

## General Information

### **Useful information about privacy settings for online platforms**

- Zoom - <https://zoom.us/security>
- Microsoft Teams - <https://www.microsoft.com/en-gb/microsoft-365/microsoft-teams/security>
- Skype - <https://support.skype.com/en/skype/all/privacy-security/privacy-settings/>

### **Further Training**

- <https://learning.nspcc.org.uk/safeguarding-child-protection/online-safety-for-organisations-and-groups> ).
- For more information about safer electronic communication: <https://www.csas.uk.net/procedures-manual/#cat-4>

For further information, please do not hesitate to contact:

Fr Paul Daly  
Episcopal Vicar for Formation  
[Paul.Daly@dioceseofsalford.org.uk](mailto:Paul.Daly@dioceseofsalford.org.uk)

Dawn Lundergan  
Director of Safeguarding  
[Dawn.Lundergan@dioceseofsalford.org.uk](mailto:Dawn.Lundergan@dioceseofsalford.org.uk)

Rachel McGee  
Communication Manager  
[Communications@dioceseofsalford.org.uk](mailto:Communications@dioceseofsalford.org.uk)

Lorraine Leonard  
Diocesan Youth Ministry Manager  
[Lorraine.Leonard@dioceseofsalford.org.uk](mailto:Lorraine.Leonard@dioceseofsalford.org.uk)