Guidance on safeguarding whilst using videoconferencing platforms for ministry

In what are unprecedented times, Covid-19 has presented many challenges to individuals and organisations. 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.

All platforms that bring people together have the potential to present a risk to users, especially children, and adults at risk, or who are otherwise vulnerable. As users of these platforms, we have a responsibility to ensure that our communications are as secure and private as they can be. This general guidance is designed to help the Catholic community across England and Wales safeguard the welfare of any person involved in activities organised in the name of the Catholic Church whilst using online platforms and social media.

Where dioceses, religious congregations and other Catholic organisations have their own policy and procedure in relation to online communication and networking this must be followed. In the absence of a local policy and procedure this good practice guidance can be followed.

General considerations when using online platforms for ministry

- It is recommended that research is undertaken in relation to safety and security concerns for the platform you choose, to enable you to consider any issues and possible alternatives;

- Be aware that different platforms have different restrictions in relation to age so ensure you take account of age restrictions within the terms and conditions of use of your chosen platform;

- 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.

- Ensure that the administrator/host is aware of the settings that will maximise security and that they are confident and competent in using them.

- Communication should always be via an organisational account and organisational equipment. A generic email address or telephone number associated with the group, accessible to more than one person who can act as administrator, maintains 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.

- 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;

- Permission for communicating directly with children and young people aged under 16 years via social media must be sought from parents;

- For young people aged 16-18 years and adults who lack capacity to consent, consent must be given by a person who has the legal authority e.g. lasting power of attorney for health and welfare, to make the decision on the person's behalf;

- Communication via social media should not be for any other reason other than the specific ministry for which consent was obtained;

- For matters that are sensitive or private, online communication should be avoided due to the possibility of misunderstanding and, if used, two adults should be present and where appropriate, parents or carers should be included where to do so would not cause harm to the individual concerned;

- Information should be circulated to parents and carers about the platform being used, including how to download the application and any key issues they need to be aware of.

- 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.

- There should be two adult facilitators during online ministry to children, adults at risk or who are otherwise vulnerable, one of whom must be familiar with safeguarding policies and procedures.

Setting up a 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 ensure you use the randomly generated ID at the time of scheduling the meeting, rather than your personal meeting ID which is given when you create an account with the choses platform;

- Ensure that your joining instructions provide information on the 'rules of engagement' which 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 rejoining 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. 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)[1];

[1] 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

- 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 the 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 position yourself in front of 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 that you 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 you have consent to share screen-shots during the meeting, ensure that the meeting 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 you do not know or have not invited into 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.

For more information about safer electronic communication see
https://www.csas.uk.net/procedures-manual/#cat-4

Useful links and resources for internet safety

The UK Council for Child Internet Safety (UKCCIS) is a voluntary organisation chaired by Ministers from the Department for Education and the Home Office. UKCCIS brings together over 180 organisations and individuals from government, industry, law enforcement, academia, charities and parenting groups. Some of the organisations UKCCIS works with include: Cisco, Apple, Sony, Research in Motion, the four largest internet service providers, Facebook and Microsoft.

The Child Exploitation and Online Protection Centre (CEOP) has numerous resources for parents and carers and children using the internet; there are several video tutorials on the THINKUKNOW site which is part of CEOP.

Lucy Faithful Foundation is a registered child protection charity which works to prevent child sexual abuse. It runs 'Stop It Now!' and 'Parents Protect.

Stop It Now! reaches out to adults concerned about their own behaviour towards children, or that of someone they know, as well as professionals, survivors and protective adults. Stop It Now! runs a Freephone confidential helpline.

'Parents Protect' is a site to help parents, carers and other protective adults with information and advice to help them prevent child sexual abuse.

Catholic Youth Work has detailed guidelines on the use of social networking sites.

Internet Matters gives advice on parental controls and is a great way of preventing children accessing unsuitable content online.

Childnet International is a multi-lingual resource site which has a guide on protecting your privacy on 'Facebook'.

The NSPCC has useful resources for keeping children safe online including sections on Cyberbullying and Sexting. Reporting and Monitoring.

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/