



Safeguarding Guidance on the use of technology / social media

JULY 1, 2020

Purpose:

Sisters of Mercy Southern Province need to assess the benefits of technology and how this can be used safely and effectively, in line with rules that respect the dignity and rights of all users, particularly children in the following areas;

- 1. Online communication**
- 2. The internet**
- 3. Texting and emailing**
- 4. Photography**
- 5. Zoom / Video calling**

The majority of occasions when people use mobile phones, computers or take photographs of children or vulnerable adults do not provide any cause for concern. However, there are occasions when this is not the case.

At the outset it is important to identify the risks associated with the use of technology, and then to minimise the risks by putting in place measures outlined below.

1. Guidance for any online communication

While there are amazing benefits to these platforms for educational, professional and personal use, some aspects need to be considered when communicating with these platforms.

Regardless of the platform being used, before sharing content or forwarding on a message to a group or other contacts, STOP and ask yourself

- “Why am I sharing this?”
- “Does this content fit within the guidelines for which this group was created?”
- “How could this content be interpreted by others?”
- “Does this content reflect the ethos of our organisation?”

*For messages that have been forwarded on to you, before re-sharing STOP, check the source and ensure the content is accurate. Again, ask the above questions.

General Advice

- The digital age of consent in Ireland is 16 years. For those under 16 years who wish to use any online service or platform which collects and/or processes their personal information, parental permission is required. Hence, WhatsApp’s minimum age increase from 13+ to 16+. For more information see Data Protection Act 2018 <https://data.oireachtas.ie/ie/oireachtas/act/2018/7/eng/enacted/a0718.pdf> and <https://www.dataprotection.ie/>

- Be mindful of requesting people especially youth to join group video chats or share video content from their home. Some may feel uncomfortable sharing their home environment. Other family members, personal information etc. may also be visible. Certain platforms enable users to use generic backgrounds when sharing video content. Encourage people to choose this option where possible and/or provide alternative means of connecting for those uncomfortable with group video chats or sharing video content.
- Update all apps as required to benefit from the latest security and privacy options.

Checklist

1. Are the platforms we are encouraging people to use Age Appropriate?
2. For those under 16 years, have I provided parents with updated information guides on the platform's we are using with youth, so they can understand the associated benefits and risks? Common Sense Media <https://www.commonsensemedia.org/> and National Online Safety UK <https://nationalonlinesafety.com/guides> offer up-to-date guides and advice regarding current popular Apps.
3. Have I informed people of the privacy settings of the platforms I am encouraging them to use?
4. Have I set clear guidelines on what is acceptable/unacceptable to share on the platforms we are using?
5. Am I connecting people through a platform who would not have been in contact previously (e.g. the creation of a group where all members now have access to contact details of all other members)? If so, have I gained consent for their personal information to be shared in this way?

Instagram. Age rating 13+ (Digital Age of Consent in Ireland is 16 years)


Instagram's Privacy Settings and Information contains instructions on how to control a number of aspects on your account including filtering out comments you do not want to appear on your posts on Instagram, turning off comments for Instagram posts and removing Instagram images from Google search. These privacy settings can be accessed in their Help Centre under 'Managing My Account'. Link <https://help.instagram.com/196883487377501>

If you are encouraging people to use this platform, it would be advisable to remind them of the privacy setting Instagram offers and make sure they know how to block (detailed instructions in their Help Centre under Privacy and Safety Centre. Link <https://help.instagram.com/426700567389543>) and how to report issues (detailed instructions in their Help Centre under Privacy and Safety Centre. Link <https://help.instagram.com/372161259539444>)

WhatsApp. Age rating 16+ (Digital Age of Consent in Ireland is 16 years)

WhatsApp Privacy settings enable you to control your visibility when using WhatsApp, who can add you to a group chat, who can see your profile picture and whether or not contacts can see if you have read their messages/or when you were last online. You can also block contacts and report issues. Link to WhatsApp Privacy Settings

<https://www.whatsapp.com/privacy>

A big issue on any online platform is the spreading of misinformation. You may have already come across a number of 'warning messages' which are circulating on WhatsApp. If a message has been forwarded on to more than 5 people, a double arrow icon will be present . WhatsApp have now introduced new stricter limits on forwarding messages.

If encouraging youth to use WhatsApp, remind them to secure their privacy settings and check out WhatsApp's advice on helping to "prevent the spread of rumours and fake news"

Link <https://faq.whatsapp.com/26000216>

2. Guidance on Use of the Internet

It is recognised that the internet is valuable and widely used. Within the Church context, clear guidelines must be developed especially for any activity involving children

The following are deemed unacceptable behaviours, and must be avoided in every situation:

- Visiting internet sites that contain offensive, obscene, pornographic or illegal material;
- Using a computer to perpetrate any form of fraud or piracy;
- Using the internet or email systems to send offensive and harassing material to others;
- Using obscene or racist language in computer-assisted communications;
- Publishing defamatory or otherwise false material generated by oneself or by others through social networking;
- Introducing any form of malicious software into the used network;
- Intentionally damaging any information communication technology equipment;
- Using another user's password, or giving that password to a third party.
- Anyone using a shared computer requires their own individual password;

3. Guidance on Texting and Emailing

Texting and email are very quick and effective methods of communication for those involved in Church activities usually this does not include adult members of Church personnel contacting young people directly, as contact is usually made via their parents/guardians.

Any Sister using this method of communication with young people / Vulnerable adults should ensure appropriate safeguards are in place as there are certain risks associated with the safe and appropriate use of texting and email, which must be managed.

The risks of text and email messaging for children/young people and Vulnerable adults are:

- ï Inappropriate access to, use of, or sharing of personal details (names, numbers, email addresses);
- ï Unwanted contact with children/young people from adult's text bullying by peers etc.;
- ï Being sent offensive or otherwise inappropriate materials;
- ï Grooming for sexual abuse;
- ï Direct contact and actual abuse.

The risks for adults include:

- ï Misinterpretation of their communication with young people/Vulnerable adults;
- ï Potential investigation (internal or by statutory authorities);
- ï Potential disciplinary action.

The following guidance is provided to minimise risk to all:

- Consent must be obtained from young people and their parents/guardians prior to sending young people text or email messages. Parents/guardians should be offered the option to be copied on texts and emails that their child will be sent.
- The young people's/vulnerable adults mobile phone numbers or email addresses should be stored safely and securely with access only available to the specific identified members of Church personnel. The numbers or details should not be shared with anyone else, and should only be used for the purposes of the text and email messaging system regarding the Church activity;
- All text and email messages sent must make it clear to those receiving them who has sent the message;
- Young people vulnerable adults should not be given the opportunity to text or email back to the system. It should only be used as a one-way communication channel;
- The text and email messages that are sent must never contain any offensive, abusive or inappropriate language;
- When this guidance is being provided in relation to Church-related activities, all of the text or email messages sent must be directly related to Church activities. The text or email messaging system and mobile phone numbers must never be used for

any other reason or in any other way;

- All of the text and email messages sent should include a sentence at the bottom that provides young people/vulnerable adults with the opportunity to unsubscribe from receiving further text and email messages.

4. Guidance on the use of Photography

The use of photos on websites and in other online/hard copy publications can pose direct and indirect risks to children and young people. We have a responsibility for safeguarding and the use of photography if we plan to use the photographs for Congregational purposes.

Risks to children

Even if the child's personal identity (full name, address) is kept confidential, other details accompanying the photo can make them identifiable and therefore vulnerable to individuals looking to groom children for abuse. There is also a risk that the photo itself will be used inappropriately by others. Photos can easily be copied and adapted, perhaps to create images of child abuse, which can then find their way on to other websites.

How to minimise risks

- Establish the type of images that appropriately represent the activity and think carefully about any images showing children and young people on the Provincial website or publication;
- Never supply the full name(s) of the child or children along with the image(s);
- Only use images of children in suitable dress and focused on the activity, rather than one particular child;
- Obtain permission: the permission of parents/guardians and children should always be sought when using an image of a young person. Parents/guardians should be aware of the Church's policy on using children's images and of the way these represent the Church or activity. This must be recorded on a joint consent form for use of images of children. The child's permission to use their image must also be recorded if they are less than eighteen years of age. This ensures that they are aware of the way the image is to be used to represent activity.

Responding to concerns

Children and parents/guardians should be informed that if they have any concerns regarding inappropriate or intrusive photography, these should be reported to the Provincial office to ensure that any reported concerns are dealt with in the same way as any other safeguarding issue.

5. Guidance on Zoom

Before Zoom meeting.

- The meeting organiser will decide the purpose of the Zoom meeting and the invitees, this will be recorded and kept on file.
- Only those invited by the organisers will be allowed into the zoom meeting.

Zoom meeting.

- Each member will sign in and enter the waiting room
- The organisers will be online and each potential member will be admitted to the meeting one at a time.
- Members faces must be visible to the organisers.
- No calls to be from bedrooms.
- Appropriate dress code for all members.
- Uninvited guests will be blocked.

Zoom Tick list

Setting up the meeting

Zoom Settings checked;

<input type="checkbox"/> Hosts video on <input type="checkbox"/> Participants video on <input type="checkbox"/> Disable "join before host" <input type="checkbox"/> Waiting room established <input type="checkbox"/> Disable private chat <input type="checkbox"/> Disable "mute participants on entry" Tick box <input type="checkbox"/> "prevent participants from saving chat" <input type="checkbox"/> Disable "auto saving" Chats <input type="checkbox"/> Enable screen sharing if needed.

Before opening the meeting

Meeting should commence with organisers 10 minutes prior to the main meeting.

- Prepare meeting objective.
- One organisers will supervise the waiting room, remind members in the waiting room to have their correct name on screen for access.

The meeting online

- The organiser will place all members' microphones on mute at the beginning of the meeting.
- Organiser or a delegated person is to supervises members' online etiquette.

- Lock meeting once all participants have joined.
- In the event of unwelcome guests, remove and block or click “end meeting”.