Sisters of Mercy
Northern Province

Safeguarding Guidance on the use of technology / social media

MARCH 12, 2021

Purpose:

The Sisters of Mercy, Northern Province realise 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 and adults at risk of harm in the following areas:-

1. **The internet**
2. **Online communication and social media**
3. **Texting and emailing**
4. **Photography**

In the majority of cases, when people use mobile phones, computers or take photographs of children or adults at risk of harm, there is no cause for concern. However, there are occasions when this is not so.
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 the measures outlined below.

1. Guidance on Use of the Internet

It is recognised that the internet is valuable and widely used. Within the Mercy context, clear guidelines must be developed especially for any activity involving children/adults at risk of harm.

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.

2. Guidance for any online communication and social media

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

Republic of Ireland

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+. *(See Appendix for more information on Data Protection Act 2018, RoI)*

Northern Ireland

If the service that you offer directly to children is an online service (in law, an "information society service" ISS), then you do need the consent of the parent/guardian if the child is under the age of 13 and in the UK (i.e. those aged 13 and older can lawfully provide consent for themselves).

Other countries in the EU may have decided on different age levels for this purpose, which can be between 13 and 16, so take care if offering online services to children outside of the UK. In Ireland the age is 16.

The Information Commissioner's Office (ICO's guidance) is clear and helpful in what you need to know about offering online services to children.

(See Appendix for more information on Data Protection Act 2018, NI)

- Great care is needed before requesting people - especially children/young people/adults at risk of harm - to join group chats, video chats or share video content from their home. Some may feel uncomfortable sharing their home environment. It is important to be aware that the use of video technology allows participant to virtually enter the space where others live and work. Other family members' personal information etc. may also be visible and there

could be a concern in respect of an individual's right to privacy.

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.

- It is important to update all apps as required, to benefit from the latest security and privacy options.

Checklist for the Service -provider
In advance of commencing online activity

1. Are the platforms I am using Age-Appropriate?
2. For those under 16 years, have I obtained the written consent of parents / guardians for use of the particular platform?
3. Have I recently checked advice and guidance regarding popular apps? e.g. Common Sense Media https://www.commonsensemedia.org/ and National Online Safety UK https://nationalonlinesafety.com/guides
4. Have I set clear guidelines on what is acceptable/unacceptable to share on the platforms I am 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?

(See Appendix for more information one-safety (NI) Data Protection Act 2018, NI)

3. Guidance on Texting and E-mailing

Texting and email are quick and effective methods of communication for those involved in Mercy activities. However, should Mercy personnel need to contact a young person the contact is usually made via parent/guardian/other responsible adult. Usually this does not include Mercy personnel contacting young people directly, as contact is usually made via their parents/guardians.

Any Sister texting/emailing young people/adults at risk of harm should ensure the communication is appropriate, safeguards are in place and that risks are managed effectively.

Risks of text and email messaging for children/young people and adults at risk of harm are:

- ï Inappropriate access to, use of, or sharing of personal details (names, numbers, email addresses);
- ï Unwanted contact with children/young people/adults at risk of harm, from adults, 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/adults at risk of harm;
- ï Potential investigation (internal or by statutory authorities);
- ï Potential disciplinary action.

The following guidance is provided to minimise risk to all:

- o Consent must be obtained from young people, their parents/guardians and adults at risk of harm, prior to sending text or email messages. Parents/guardians should be copied into texts and emails that their child will be sent.
- o The young people's/adults at risk, mobile phone numbers or email addresses should be stored safely and securely with access only available to the specific identified members of Mercy personnel. Personal 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 Mercy activity;
- o The identity of the sender/author of text and/or email message should be absolutely clear to the recipient.
- o The text and email messages that are sent must never contain any offensive, abusive or inappropriate language;
- o All of the text or email messages sent must be directly related to Mercy activities. Text or email messaging system and mobile phone numbers must only be used in direct relation to the ministry activity or for the primary purpose for which the communication was set up.
- o All of the text and email messages sent should include a sentence at the bottom that provides young people/adults at risk of harm with the opportunity to unsubscribe from receiving further text and email messages.

- Clear guidance should be provided on the use of mobile phones during activities and especially on the use of mobile phone cameras which can be easily used for offensive actions without the subject being aware of their use.

4. Guidance on the use of Photography

The use of digital, electronic or hard copy photographs of any person and in particular of children, young people or adults at risk of harm can pose both direct and indirect risks. The Sisters of Mercy have clear guidelines for the responsible use of photographs for Congregational purposes. This is deemed to be a safeguarding matter and all are asked to adhere to the protocols

Risks to children/young people/adults at risk of harm

Even if the person's personal identity (full name, address) is kept confidential, other details accompanying the photo can make them possibly identifiable and therefore vulnerable to individuals who may wish to groom them for abuse. There is also a risk that the photo itself will be used inappropriately by others. Photos can easily be copied, adapted or photoshopped for a myriad of purposes and 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/young people or adults at risk of harm, on the Provincial website or publication;
- Never supply the full name(s) of the child/children/young people/adults at risk of harm along with the image(s);
- Only use images of children/adults at risk of harm in suitable dress and focused on the activity, rather than one particular individual;
- Obtain permission: the permission of parents/guardians/children/adults at risk of harm, should always be sought before using their image;
- Inform oarents/guardians of the Mercy policy on using children's images and of the way these represent the Mercy 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, parents/guardians/adults at risk of harm, 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.

Appendix: Useful References

ROI: Digital age of consent - 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/ and www.gov.uk/data-protection

ROI: Ireland's Official Online Safety Hub
www.gov.ie/en/be-safe-online

Instagram. Age rating UK 13+ (Digital Age of Consent in Ireland is 16 years)
https://help.instagram.com/196883487377501

WhatsApp. Age rating UK 16+ (Digital Age of Consent in Ireland is 16 years)
https://faq.whatsapp.com/26000216

NI: Digital age of consent- See Information Commissioner's Office and/or
https://www.nicva.org/data-protection-toolkit

Child Exploitation and Online Protection Centre (CEOP), https://ceop.police.uk,

The UK Safer Internet Centre, https://www.saferinternet.org.uk

The Safeguarding Board N.I. https://www.safeguardingni.org/esafety

Childnet, https://www.childnet.com