Safeguarding & Digital Technology

Tipsheet: Safe use of Online Platforms in our Work

Designing for Safety

Save the Children increasingly designs and implements programs and advocacy campaigns that use digital technology and social media to engage and empower children, young people and vulnerable adults and to support their participation and development. Information and Communication Technologies (ICT), including commercial digital platforms provide substantial benefits for our stakeholders. They enable access to information, resources, communication and support and can help children access their rights to information and participation. However, they can also come with substantial risks, including online abuse, misuse of data, and others.

Although Save the Children has strong Safeguarding policies, procedures and practices, and child protection programming ,approaches and guidance , digital technologies change rapidly, and innovative uses of technology often give rise to new and emerging risks. Because the rights, protection and safety of our program participants is our priority, our risk appetite is low, even when we are innovating with new ways to use technology and data. We must uphold our commitment to understand and minimise avoidable risks as we promote innovation in a rapidly evolving digital landscape. We must also ensure data privacy and protection, particularly in relation to children, adult program participants, and their families (see the SCI Data Protection Policy).

Risk assessment and mitigation strategies are a critical part of the program design phase, and they should be revisited throughout program implementation as well as when there are context changes. In this Tip Sheet you will find guidance to support proposal writers, program designers and implementers, (including thematic teams, MEAL, Advocacy and Campaigns) who are considering the use of online platforms (such as social media and messaging apps) in their programs.

Teamwork and Collaboration

Country Offices are responsible for assessing and identifying risks to participants in any Save the Children programs and putting appropriate measures in place to safeguard children, young people, and vulnerable adults, as well as staff and volunteers. Child Protection, Digital Technology architecture, IT, Safeguarding, Legal, Data Protection and other relevant colleagues should collaborate to put mechanisms in place to respond to and manage any concerns raised online or potential risk to a child. Awareness, prevention, reporting and response interventions should be included in the design and reporting and response procedures as required.

What is Online Abuse?

Online Abuse is any form of abuse that happens via the internet. It can take place on any online platform or device that is connected to the internet, such as computers, tablets and mobile phones. Anyone can suffer online abuse or harassment, but its intensity and nature can differ based on context,, age, sexual orientation, gender identity and expression, disability status or other social characteristics of the victims.

Online Risks and Harms:

Online risks and harms are often divided into five categories:

1) Content risks: risks related to content that can be found online, such as hate speech, sexually exploitative images and videos of children, adult sexual material, violent content, discriminatory material, images or videos that promote self-harm, and radicalising material amongst others.
2) Contact risks: risks that are the results of others' online behavior, such as cyber bullying, harassment, grooming, sex trafficking, radicalisation, and distributing private and sexualised images and sexting.
3) Conduct risks: risks that are the result of people's own online behavior which might put themselves or others at risk, such as connecting with unknown people online, unintentionally revealing their identity or location, creating and sharing sexual or otherwise private materials and failing to secure a device.
4) Consumer risks: risks that come from marketing to children, online profiling and manipulation through marketing techniques, financial risks such as advertising or fraud, exposure to harmful products, and the possibility of identity theft.
5) Crosscutting risks: risks related to loss of privacy through data, advanced technologies such as the use of artificial intelligence and predictive analytics that can exclude children now or in the future from accessing their rights and vital services, and corporate or government surveillance.

Staff Use of Online Platforms

Save the Children staff generally use social media and messaging apps for four primary reasons:

1) Corporate communications: SCA's Fundraising, Campaign and Communications staff use social media channels for organisational fundraising to position Save the Children's brand in the marketplace and to drive Sponsorship and donations. Campaign and communications staff use social media and other platforms to engage supporters, decision makers and children. Social media platforms, including Linkedin , Twitter, Facebook , Instagra Pinterest and YouTube ,, , and are major channels for SCI's fundraising, campaign and communications activities. Communications staff have special training, guidance and authorization to post content on social media channels. Other staff are encouraged to "like" and share those official posts.

2) Personal communications: Save the Children staff worldwide often post to online platforms or send messages about their work to non-Save the Children staff because they are proud of that work and want to educate friends or the general public about the lives of our program participants. These personal communications can be an effective way of garnering support for Save the Children and our work because they tell a story from a personal point of view to friends, family, colleagues and peers.

   They also have the potential to put program participants – and sometimes staff and volunteers – at substantial risk. For this reason, all employees and volunteers are required to follow a strict policy regarding the use of social media to communicate about our work. Refer to the IT security and data protection guidelines for usage of social media and the Social media policy. For further guidance on personal usage of social media and guidance for managers on policy breaches, please refer to this page.

3) Business operations communications: The SCI Information Technology team has identified secure applications – such as Microsoft Office 365, Outlook, OneDrive, SharePoint (OneNet), Workplace and Microsoft Teams – to be used for our business communications. IT staff have configured these applications as well as our computers, connectivity, and storage systems to be secure and actively maintains that security by applying software upgrades, defending our servers from malware and hacking attempts, removing access rights from past employees, backing up all files and similar measures.

   For those reasons, all Save the Children business communications should occur using the applications that have been pre-approved and configured by the IT team and not through personal email accounts, messaging apps, social media platforms or other tools. For more information or support, contact the SCI IT security help desk.

   Before using your own computer, laptop and phones, special authorisation must be received from the Country or Regional Director or Head of Function. Refer to SCI's Bring Your Own Device (BYOD) policy. It is recommended that any official contact with program participants be done through an official SCI number. In situations where this is not possible, you must ensure risks are assessed and safety measures are put in place and known by staff and management, and you have adhered the BYOD policy. If working with volunteers, additional risks must also be assessed to decide whether this is the best course of action.

   Even if Save the Children co-workers are "friends" or contacts with each other on a social media platform, (such as, but not limited to, Facebook, Instagram, LinkedIn or Twitter) or a messaging app, (such as, but not limited to, WhatsApp, Viber or Snapchat) and are accustomed to communicating with each other via those platforms, they **must** use the platforms provided by the IT team for business communications, whether or not the content of those communications is sensitive. It is ***never allowable*** to discuss confidential information or information that would allow any program participant to be identified over platforms that have not been approved by the Save the Children IT department. Refer to the SCI Acceptable use of IT policy and online courses, the IT security training and data protection awareness training which explain your obligations when using SCI's IT systems.

4) Use in humanitarian or development programs: Because mobile phones have become ubiquitous, even in many of the Least Developed Countries where Save the Children works, several social media and messaging platforms have grown a massive global user base.

   Some Save the Children programs accept the risk in order to take advantage of that existing user base – including Facebook's more than 2.6 billion users and WhatsApp's more than 2 billion users worldwide – to communicate with their program participants or other stakeholders for activities such as Behavior Change Communications (BCC) or Risk Communication and Community Engagement (RCCE).

Currently, WhatsApp, Facebook and other platforms are being used in several Save the Children program, advocacy and campaign activities. A few examples include:

- The Peru country program established a WhatsApp group for cash transfer activities.
- The Kosovo country program and UNICEF supported the Ministry of Education to develop and launch an ECCD platform to support children and their parents.
- The Mozambique country program carried out a rapid consultation through the Young MPs' WhatsApp group to gather children's views on COVID-19.

The benefits of using online platforms, for example messaging platforms, to communicate with large numbers of program participants, and in the context of our humanitarian response or crisis situations, may be considerable. However, their use should be risk-assessed for each specific situation and balanced with the functionality and benefits that they offer. This provides an opportunity to identify technical and operational controls to mitigate some of the risk. Where needed, the Data Protection team can assist with conducting a full Data Protection Impact Assessment (DPIA). Contact the Data Protection Officer dpo@savethechildren.org to have an initial discussion or review guidance on DPIAs on OneNet.

Because SCI's IT team has no control over these platforms, how people use them, who is connecting through them or whether the people using them have configured them to be secure or not, they are inherently riskier than our corporate communications systems. Because they are designed to communicate with large numbers of people – who are often unknown to each other – social media and messaging platforms such as Facebook and WhatsApp pose a high risk for children and other program participants, including risks of abuse and exploitation, disinformation, and privacy violations. Most of these are inherent to the platform, our responsibility is to understand and reduce risks however, we cannot prevent it entirely.

To enable those risks to be identified and to get advice on mitigating or accepting those risks, program teams should conduct a full Data Protection Impact Assessment (DPIA). The Data Protection team can assist with this.

If, following a DPIA, a decision is taken to make use of social media or messaging platforms, the Social Media Risk Mitigation Tool can offer program teams basic mitigation strategies for safeguarding risks. MEAL, T4D and safeguarding teams should be involved when Country offices are considering using digital and messaging platforms as part of feedback and reporting mechanisms and other accountability interventions. Please refer to the Feedback and Reporting Channel Tipsheet.

If Save the Children is reporting a concern to an external agency (ex: government, NGO or UN), we must ensure that we do this safely and do not breach confidentiality or data protection or any other rules and regulations.

To use messaging apps such as WhatsApp as part of our safeguarding reporting channels, staff must ensure an official Save the Children number is being used. If a report is received through WhatsApp, the information must be properly documented and uploaded onto Datix. Safety measures must be in place to ensure no breach of confidentiality, data protection or risk to the person reporting. All safeguarding concerns no matter how initially received need to be uploaded onto Datix Cloud. For the management of safeguarding cases, **Datix cloud,** our online case management system, must be used.

Safeguarding Risks

It is important to identify and assess risks with the specific platforms and usage when deciding whether it is appropriate to use online platforms in the context of delivering our programs. This list is not exhaustive.

General Safeguarding Risks

- Safeguarding is not adequately considered when designing, budgeting, staffing and implementing programs through digital technology, social media, and messaging platforms to prevent avoidable risks
- Online programming started before safety measures, procedures, guidance, and other learning materials have been developed and implemented at all levels
- Increased online activity by staff, volunteers and partners increases the risk of online abuse against program participants and violations of data protection
- Poor understanding of safeguarding risks or incidents associated with digital technology
- Lack of law enforcement and limited ability to respond in a system when the local laws do not include online crime, ex: online child abuse

The Social Media Risk Mitigation Tool helps teams working with the social media and messaging

platforms most commonly used at SCI to identify key child safeguarding risks and adopt strategies to mitigate those risks. Additional guidance on how to mitigate the risks is provided below.

How to mitigate risks?

The following are safeguarding good practices for staff using digital technology, social media and messaging platforms to reduce the risk of online abuse in Save the Children programs and to use these platforms safely. This list of mitigations is not exhaustive and you must identify the risks and mitigations for the specific platform and purpose.

Assess risks and develop mitigation strategies

- ✓ When using any social media platform or messaging application in Save the Children programs, use your judgment: anticipate what can go wrong so you don't put children at risk
- ✓ Conduct a safeguarding and IT security and data protection risk assessment to identify, mitigate and manage risks
- ✓ Map-out current and potential use of social media and messaging platforms alongside a risk assessment before deciding on which platform to use

Assign budget, responsibility, and accountability

- ✓ Make sure everyone within your country office knows who is responsible for monitoring and moderating the content of the websites, social media platforms and social networking areas and how to contact them
- ✓ Budget for digital technology/ICT expertise to support design and application of digital technology innovation in programs and appropriate training for staff, volunteers, partners and program participants: for example, online safety, safe use of social media and messaging platforms, and moderation
- ✓ Budget for moderation of chat functions, forums, or comments sections established when using social media platforms. Ensure appropriate SOPs and guidance have been developed and disseminated
- ✓ Build in reporting and response mechanisms for children and other program participants to report safeguarding concerns, whether online or offline
- ✓ Put in place a process for feedback, review, and improvement for the use of the platform
- ✓ Remember that Save the Children is responsible for all content contained on its website, forum blogs, tweets or social networking areas; regularly monitor the sites.

Strengthen awareness and capacity

- ✓ Make sure staff operating the Save the Children social media accounts and moderating groups and forums have been trained on how to identify and respond appropriately and respectfully to safeguarding and safer programming concerns that are shared through social media and how to report any safeguarding incidents
- ✓ Ensure that children, young people and other program participants in Save the Children programs who use the platform have received at least basic child-friendly online safety instruction
- ✓ Provide links to additional online safety information and resources to children, young people and other program participants so they can educate themselves about internet safety and risks
- ✓ Ensure that children, young people and other program participants know who and where to report to if an SCI employee makes unauthorised contact (e.g. using a personal email address or sending a direct message)
- ✓ Ensure staff and moderators can identify inappropriate online behaviors such as grooming, signs of abuse and other risks. Refer to resource section below
- ✓ Staff should not be anonymous while communicating with program participants. Name and job title must be provided unless the activity is set up to generate general responses from the program and not an individual staff person

Follow policy and procedures

- ✓ Communicate only from Save the Children-owned social media and messaging accounts, not from the accounts of individual staff members. Ensure that the login credentials of all accounts are saved in project documentation and change account passwords when the staff using those accounts change. If using a personal account, then there must be documented authorisation
- ✓ Create SOPs on the use of devices by program participants in any of our centers, shelters or safe spaces managed or supported by Save the Children. These should include how usage is monitored and how users should be supervised
- ✓ Supervise and monitor use of digital and social media platforms in programs to ensure that no content in breach of SCI data protection policies/regulations is posted, including but not limited to confidential information, personal data, harmful content or copyrighted content is posted. This includes managing accounts and setting up a mechanism to report and

remove any sensitive information or inappropriate content that could breach data protection rules

- ✓ Communicate with children and young people in groups and not in isolation for activities related to child participation and engaging with children where the two staff rule would apply in a physical environment. If sending out group messages or using social media such as Facebook for campaigning or to solicit children's views, this must be done on official Save the Children accounts and proper monitoring and safety measures put in place
- ✓ All communication with program participants must be work-related and conducted through approved channels
- ✓ Set up a group agreement with children and young people about expected behaviors for the sessions from themselves and the adults facilitating the session as well as the consequences of violating the agreement. Have clear procedures and a code of conduct in place
- ✓ Require staff and volunteers who come into contact with children through digital platforms to undergo background checks just as they would if they were coming into physical contact with children in our programs
- ✓ Reinforce existing policies to staff and volunteers, including the Acceptable use of IT policy, Social media policy and, Child Safeguarding policy, PSEAH policy and the Anti-Harassment, Intimidation and Bullying policy and the Code of Conduct
- ✓ Do not post or host items which may be considered to be hurtful, insulting, offensive, abusive, threatening, racist, discriminatory or otherwise may cause offence or harm to another or might incite such behaviour in others

Protect privacy and confidentiality

- ✓ Staff operating the Save the Children social media accounts should not share information from messages they receive (including personal data) with colleagues, other than those authorized. Check the Feedback Handling Standard Operating Procedure (SOP) annex 3 in this document
- ✓ Keep location private. By default, many mobile phones save the GPS location and other information with every photo taken. To avoid sharing these details when sharing a photo, turn geo-tagging off on the camera on any mobile phone (Check out tutorials for iOS and Android)
- ✓ Do not exchange personal e-mail addresses or social media accounts (for example, Facebook, Snapchat or Instagram) with program participants. If a program participant sends a friend request, do not accept it. When engaging with program participants, remind them of the rules and regulations to reinforce this

Don't make assumptions

- ✓ Many social media sites offer tools that attempt to moderate comments added by users. For example, they might automatically remove comments that contain swearing or foul language. Do not rely on 'automated digital moderation tools' on social media platforms or forums when soliciting comments from target groups, as tools have been found to be problematic and cannot be relied upon as an effective tool for moderating users' comments.
- ✓ Do not assume that children, young people and adults know the rules
- ✓ Do not assume that access to a mobile device implies that the child, adult or young person is digitally literate

For further information and support contact:

Safeguarding

Susan Grant, International Safeguarding Director Susan.grant@savethechildren.org
Regional Safeguarding Directors.

IT

Deborah McManamon, Data Protection Officer dpo@savethechildren.org
IT Security: itsecurity@savethechildren.org

Save the Children resources:

Safeguarding Risk Assessment & Risk Directory.xlsx

SCI Safeguarding and Social Media Guidance
English, Arabic, French and Spanish

SCI Field-Friendly guidance posters
English, Spanish & French

A handbook for grown-ups on how to protect children from sexual abuse on the internet (SC Sweden)

Save the Children #YouThinkYouKnow campaign for children and parents

Save the Children #SafeWeb4Kids Children's guide to online safety

Operational Handbook for Child Online Safety Centres

The Principles of Interacting with Children in Chat Work

Best Practices in Support to Child Victims of Violence in the Digital Environment

External resources:

Age-Appropriate Design: A Code of Practice (UK Information Commissioner's Office)

Principles for Digital Development

ITU cyber security for global online safety advice for parents and carers – Covid-19 pack Arabic | Chinese | English
French | Russian | Spanish

UNICEF Tips for parents and caregivers: Keeping children safe online during the COVID-19 Pandemic

Better internet for kids: multilingual resources

Think U Know information and resources

NB: Please note that the reporting links in some of these documents may not be appropriate for your Country Office.

Appendix

Data Protection Risk & Messaging Platforms

In the course of our work to support children, families and communities, SCI relies on many different technologies, devices, and communication channels.

Because of their already widespread use, their ease of implementation, and the potential to reach large numbers of people at low cost, the use of messaging platforms such as WhatsApp, Messenger and Signal by humanitarian organisations is well established.

However, just like any other technology, the risk of messaging platforms needs to be assessed in each specific situation, and the configuration, implementation and ongoing management needs to be done in accordance with SCI policies and standards. This will support the organisation in leveraging the benefits, while controlling the risk.

Some key points to consider are:

- **Service offer:** Some platforms have personal, business and corporate tiers of service which offer different levels of functionality
- **Control:** For 'free' platforms, we have no control over functionality, security or the data generated. We have no control over the platform provider's use of the data, or onward transmission of the data
- **Program Participants' rights:** How can we facilitate participants exercising their data rights (such as right to erasure of their data) – and how can we meet our corresponding duties to follow the data protection principles?
- **Program Participants' anonymity:** In some countries, additional info is gathered when users sign up to apps, and they won't be able to use them anonymously
- **Additional processing**: As well as the data that is being directly provided by users – there is also certainly going to be other data gathered or generated (e.g. metadata, location data, status, contact matching, user profile, device type). Users may not be aware of the extent of the data being gathered when they use an app or online service
- **Encryption:** Content may be encrypted on some platforms, but not all do this automatically. Metadata is not usually encrypted. Content is still vulnerable to other cyber threats
- **Multi-media:** As well as text, functionality to transmit audio, pictures, video, live stream – does this pose additional risk?
- **Disclosure:** Do we know how the platforms respond to disclosure requests for (for example) security agencies? Do they publish transparency reports?

These risks should be assessed *before* processing begins – that is, before the personal data is gathered or used. The Data Protection Impact Assessment process can help to identify the risks and mitigations and will help SCI demonstrate accountability. Please contact the Data Protection Officer dpo@savethechildren.org to have an initial discussion.

There is further guidance on DPIAs on OneNet.