WORKING WITH CHILDREN ONLINE GUIDELINES

INTRODUCTION

PREAMBLE

As we navigate this digital age and work to stay connected through online platforms, it is important to consider best practices to keep people safe online, especially the vulnerable. This refers to children, as well as other vulnerable groups, including people with disabilities.

We are aware that the online spaces can be filled with great advantages, as well as some dangers. Therefore, we must have clear guidelines in place to protect children and other vulnerable people.

Definitions:

Children: Anyone under the age of 18.

Online Communication: communicating through the internet. This includes, but is not limited to, social media platforms, messaging applications, email and video calling.

Examples: Facebook Messenger, WhatsApp, Line, Zoom, Skype, Facetime

Digital Communication: Communicating through any digital form of technology.

Examples: Phone calls, text messaging, online communication, radio, television.

Online/Cyber bullying: Using online communication to bully someone.

Examples: Sending intimidating or threatening messages, posting rumours, sharing contact details without permission, hate speech.

Online Exploitation: Using online communication to coerce, manipulate or deceive a child into sexual or criminal activity.

Example: An adult may pretend to be a young girl to convince a boy to send sexual photos to them. The adult may then use these photos to blackmail the child into sending more pornographic material.

Online Grooming: Using online communication to build trust and rapport to prepare a child for sexual exploitation.

Note: Throughout these guidelines we will refer to online communication, however these guidelines also apply more broadly to all forms of digital communication, including phone calls.

OUR COMMITMENT

We are committed to:

- working together with our partners and field workers to ensure that all our online communication with children is safe and appropriate; and
- helping educate children and families around the dangers of being online and to help them develop the skills to protect themselves online.

PURPOSE

These guidelines aim to:

1. demonstrate ACCI's commitment to ensuring safe online communication with children;

2. outline the expectations and responsibilities of any ACCI stakeholders; and
3. provide guidance to stakeholders on how to meet good practice standards.

STANDARDS & GUIDANCE

ACCI have an obligation to act within the laws of the countries wherein we operate, as well as to hold duty-bearers within those countries accountable for communicating safely and appropriately with children online.

Partners are also strongly encouraged to follow all the company standards and guidelines of any online platform they are using (see below for more details).

Please also refer to:

- ACCI's Child Safeguarding Policy
- ACCI's Complaints Handling Policy

SCOPE

All stakeholders listed below SHOULD NOT be interacting online with children who are a part of any ACCI programs, including programs run by strategic partners:

- All ACCI Staff including but not limited to employees, contractors and consultants.
- All ACCI Volunteers including but not limited to office and event-based volunteers.
- All ACCI Field Workers*.
- All ACCI Associates*.
- All ACCI Board Members.

**In some cases there may be exceptions, however we would strongly recommend that field works/associates avoid online communication with children without the supervision of a guardian or other worker, due to the power imbalance within the relationship and/or language and cultural barriers. If a field worker or associate are considering communicating online with a child, they should contact ACCI's CPO for approval and so amendments can be made to their commitment to ACCI's Child Safeguarding Policy's code of conduct.*

Those who fall within the scope below are required to read, sign and adhere to the ACCI Working with Children Online Guidelines.

- All ACCI Strategic Partners who are interacting with children online. This includes any organisation receiving ACCI funding in Australia or abroad to implement activities including but not limited to community development, disaster response or non-development activities.
    - We would strongly recommend that interaction with children online be kept at a minimum, limited to staff who are social workers, case managers or health care workers.
    - Children/Youth Ministry workers may also be engaging with children in their programs. Organisations or ministries must have high standards outlined in guidelines and code of conducts. Supervision and parental/guardian permission is essential in

these situations, especially as the line between a professional relationship and a personal relationship can be unclear. Please contact the CPO for support to develop these processes.

PREVENTATIVE ACTIONS

This section outlines the proactive measures and strategies needed to ensure ACCI's staff, operations and programs not only protect children and avoid harm online, but also promote the wellbeing and best interests of children.

COMMUNICATING WITH CHILDREN ONLINE

ACCI is committed to helping stakeholders ensure that appropriate preventative measures are in place to:

- ensure online communication within programs is child safe and appropriate;
- prevent child abusers, sex offenders or scammers from seeking to harm the children within our programs using online platforms.
- educate children in our programs around cyberbullying, image-based abuse and the distribution of harmful content

ACCI is committed to helping stakeholders meet these expectations through:

- providing training and capacity building opportunities;
- information sharing; and
- ongoing coaching and support.

MINIMUM EXPECTATIONS

The following expectations directly relate to all those who are working directly with children online. ACCI stakeholders have a duty of care when working online to take reasonable steps to protect children from any harm that should have reasonably been foreseen

In order to prevent harm, implementing partners must:

- ensure that all staff read, sign and adhere to the standards outlined in these guidelines;
- online risks need to be included in ongoing child protection risk management processes;
- train their staff about how to appropriately communicate with children online;
    - This includes developing and disseminating a clear reporting process for any concerns that arise during online activity (see Responsive Actions section).
    - Guidelines are also needed to establish boundaries. For example, staff cannot talk to children between sessions unless it is an emergency.
- assign a focal person with the responsibility of helping the organisation to adhere to these standards. This could also include assigning a team to champion online child safety within the organisation; and
- supervisors should do spot check on staff's interaction with children online to ensure boundaries are being kept.

Before communicating with a child online, staff must:

- inform their manager about what communication they will be having with children online; and

- at all times, inform parents/guardians about any online communication with their child.
- If possible, signing up for services using work email addresses and phone numbers. Avoiding giving children your personal contact details and change privacy settings so children cannot view personal social media activity.

When communicating online with children, staff must:

- use appropriate online platform tools (see Online Platform section below) and avoid using social media platforms where content, like photos and videos, can be posted. For example, never like or comment on a child's Facebook post. Limit interactions to only messaging and calling;
- if possible, use work phones and computers when communicating online with a child;
- maintain a safe and professional environment to the best of their ability;
    - We strongly recommend that there be two staff members on each call or added to every messaging chains for accountability.
- consider privacy/confidentiality when communicating online;
    - Making sure that no one is overhearing confidential conversations.
- create boundaries so that communication stays work related;
    - Write clear guidelines outlining the boundary between building rapport and communicating inappropriately.
- write detailed case notes each time you communicate with a child, which should be overseen by your supervisor; and
- when you no longer need to communicate with the child as part of your work role, end future communication and delete their details from any of your online platforms.

When working in a group call setting, staff must:

- have two unrelated team members to host and moderate the group;
- ensure that links to any online meetings be not posted anywhere publicly, but sent only to those invited to the group;
- educate the children at the beginning of a session around online etiquette and expectations;
    - Including how to treat each other during the call and what information is appropriate to share.
- disable any private chat functions;
- staff must ensure that all children have left the group call before they leave so that children cannot stay on the call and communicate unsupervised with each other.

We discourage staff from engaging groups of children in group messaging as children can continue to message each other unsupervised. This can lead to cyberbullying or sending of inappropriate content or information.

BEST PRACTICE

To comply with best practice, ACCI partners should:

- develop their own guidelines around communicating with children online;

    - This could be included in a Child Protection/Safeguarding policy, HR documents or separate guidelines.
    - It is important that staff sign an agreement or code of conduct agreeing to the organisations policy.
- consider the needs of all children including those with disability or others who may be more vulnerable and susceptible to online harms.
- session could be recorded for transparency and accountability so that there is evidence if there is any accusation of harm. However, partners must exercise extreme caution if they do record any communication with children, including gaining parent/guardian permission and ensuring the content is secure.

ONLINE PLATFORMS

It is important to choose the right online platform for communicating with children online to help reduce the risks of harm. This includes making sure that the platform is age appropriate.

Age restrictions: Most online services have a minimum age restriction in place. We strongly recommend that partners do not engage with children on these platforms if that child does not meet the age restrictions. Many platforms have restrictions in place to protect children from certain inappropriate content, therefore if children lie about their age when signing up to these platforms, they may not be protected by these safeguarding restrictions.

Examples:

WhatsApp:

- Age restriction: 16+
- Appropriate for: Individual messaging, calling and video calling
- Ways to reduce risk: Avoid group messages and calls so that children can't get the contact details of other children.

Facebook (including Facebook Messenger)

- Age restriction: 13+
- Appropriate for: Individual messaging, calling and video calling
- Ways to reduce risk: Messenger Kids, is a child friendly alternative to the main Messenger app that allows parents or guardians to review the people with whom a child connects with. Avoid group messages and calls so that children can't get the contact details of other children.

Line

- Age restriction: 12+
- Appropriate for: Individual messaging, calling and video calling
- Ways to reduce risk: Avoid group messages and calls so that children can't get the contact details of other children.

Zoom

- Age restriction: 18+ to create an account (however, children can be participants in supervised meetings)
- Appropriate for: Individual or group video calling

- Ways to reduce risk:
    - Only allow users to join meetings within your organisations account;
    - Enable the waiting room function so no one can join a meeting unless the host allows them;
    - Learn how to use the extra meeting security functions so you can use them if necessary, including:
        - locking a meeting;
        - expelling a participant;
        - preventing participants from screen sharing;
        - disabling video; and
        - muting participants.

SUPPORTING CHILDREN ONLINE

It is important to educate children to prevent child abusers, sex offenders or scammers from seeking to harm children online. We can also educate children in our programs around cyberbullying, image-based abuse and the distribution of harmful content. The following guidelines directly relate to how we can best educate children and parents/guardians.

Online Grooming:

Encourage parents/guardian (or other duty bearers) to:

- make children's accounts private and to delete contacts they don't talk to or don't trust;
- stay involved in the child's digital world;
- establish safety rules for meeting online 'friends';
- contact local authorities or organisations/helplines legally mandated to receive reports if the child has been exposed to any risk.

Encourage children to:

- report and block/delete requests from strangers;
- tell their parent/guardian if an adult is messaging them;
- be alert to signs of inappropriate contact;
- seek help and support from a trusted adult immediately if a problem arises which could be their parent/guardian, teacher, social worker or a support hotline.

Online Pornography:

Encourage parents/guardian (or other duty bearers) to:

- stay engaged and talk regularly with their children about what they are doing online;
- use parental controls on devices and ensure the 'safe search' mode is enabled on browsers;
- have an age-appropriate discussion about the issue of pornography with their children;
- respond calmly if their child has found pornography;

    - listen, assess and be sensitive to the child's feelings
- contact local authorities if the child has been exposed to any risk; and
- connect children to counselling and support services if needed.

Encourage children to:

- Talk to a trusted adult immediately if a problem arises which could be their parent/guardian, teacher, social worker or a support hotline.

Media, Misinformation and Scams:

Encourage parents/guardian (or other duty bearers) to:

- use safety, security and privacy settings on devices, games and apps at an age-appropriate level;
- teach children around how to spot and avoid online scams; and
- ensure that children know where they can turn to for help.

Cyberbullying:

Signs of cyberbullying

Child appears to be:

- emotional and upset during or after using the internet/phone;
- very secretive or protective of one's digital life;
- withdrawn from family members, friends, and activities;
- avoiding school or group gatherings;
- not doing well in class and is "acting out" in anger at home;
- shows changes in mood, behaviour, sleep, or appetite;
- wanting to stop using the internet;
- being nervous or jumpy when getting an instant message, text, or email; and
- avoiding discussions about online activities

Encourage parents/guardian (or other duty bearers) to:

- talk to their child about cyberbullying before it happens;
- listen, think and stay calm if their child is facing cyberbullying;
- talk to the child gently and help them to understand the situation and what is best to do; and
- ensure that their child knows where they can turn to for help.

Sending sexual photos and content

Encourage parents/guardian (or other duty bearers) to:

- talk to the child about how to stay connected with friends and loved ones in safe and age-appropriate ways;
- talk about the risks including what can go wrong and the legal issues;
- promote self-confidence and that it is OK to say 'no'; and
- teach children about consent and respectful relationships

If a child's intimate image is shared online

- Stay calm and open
    - reassure them that you will work through this together
- Listen, and act fast
    - work quickly to remove the content online by reporting the image to the site or service it was posted on. There may be a hotline or service in your country to support you to remove images.
- Get help and support [1]

[1] For more information on how to support children online please refer to https://www.esafety.gov.au/parents/big-issues/cyberbullying

RESPONSIVE ACTIONS

This section outlines ACCI's process and procedures for responding to child safeguarding reports, incidents and allegations that occur online.

REPORTING PROCEDURES

What do I need to report?

ACCI expects that all stakeholders will report the following:

1. Any belief or suspicion of abuse or exploitation:

- If you have reasonable grounds for belief or suspicion that a child has been abused, exploited or exposed to image-based abuse, cyberbullying or illegal and harmful content.
- If anyone in your organisation, or one of your partner organisations, are accused of, charged with, arrested for, or convicted of criminal offences relating to child abuse or exploitation. This includes if they are accused of acting inappropriately with a child online.

2. Non-compliance or failure to safeguard children:

- Non-compliance with these guidelines and/or the ACCI Child Safeguarding Policy, by someone covered under the scope of these policies.
- Activities or practices, including online, in ACCI activities that do not protect the best interests of the child (fail to implement reasonable child safeguards) or do not meet applicable local laws or standards.

3. Concerns regarding the safety and wellbeing of a child:

When there are serious concerns about the wellbeing of a child which may warrant intervention or support from child protection or social service providers. This includes if a child discloses harm during online communication.

4. Concerns specifically around a child's behaviour during online communication with a staff member:

- When a child sends an inappropriate message or makes inappropriate comments during your online communication.
    - This includes sending or saying things that may have a sexually connotation.
- Evidence that cyber bulling has occurred during a group call or as a result of a group call.

Who needs to report?

Every ACCI stakeholder is required to report incidents, beliefs or suspicions that they become aware of as described above.

How and who do I need to report to?

How an incident is reported is dependent on numerous factors, including where the incident occurred, if it involved in any way an ACCI stakeholder, project or funded activity and the type of report being made (e.g. abuse, concern regarding wellbeing, non-compliance issues).

Please refer to the ACCI Child Safeguarding Policy for more information about how or who to report to.

If you are unsure about anything regarding reporting, please contact the ACCI Missions & Relief Child Protection Officer who will be able to advise you.

Contact Details

ACCI Missions & Relief Child Protection Officer:
Email: childprotection@acci.org.au
Phone: 1300 997502 or +61 3 8516 9600
Mail: 5/2 Sarton Rd, Clayton, Victoria, Australia, 3168

If the allegation is against the Child Protection Officer, reports can be directed towards the

ACCI Missions & Relief General Manager:
Email: complaints@acci.org.au
Phone: 1300 997502 or +61 3 8516 9600
Mail: 5/2 Sarton Rd, Clayton, Victoria, Australia, 3168

RESPONDING TO CYBER ABUSE DIRECTED AT STAFF

Partners need to be aware that their staff may also experience cyber abuse during online communication. Less respect may be shown during online communication due to online frustrations and potential misunderstandings. People may also feel more confident to be abusive online then they would otherwise be face to face.

Managers should:

- respond promptly and seriously to all allegations of cyber abuse directed at staff;
- support staff who have faced abuse:
    - This could include proving supervision, counselling and/or strategies for future online communication.
    - If necessary, re-arrange workloads so that staff member does not need to communicate with the child who has been abusive.
- encourage all staff to maintain their privacy online:
    - This could include having separate accounts so that abuse does not occur on private accounts and so staff can switch off work account outside of work hours.

FURTHER INFORMATION

RESOURCES

Resources for online communication:

- https://www.unicef.org/media/67396/file/COVID-19%20and%20Its%20Implications%20for%20Protecting%20Children%20Online.pdf
- https://aifs.gov.au/cfca/publications/online-safety (Australian context)
- https://www.unicef.org/coronavirus/keep-your-child-safe-online-at-home-covid-19
- https://www.unicef.org/press-releases/children-increased-risk-harm-online-during-global-covid-19-pandemic
- https://www.esafety.gov.au/parents/big-issues/cyberbullying (Australian context)

Resources for virtual monitoring:

- https://bettercarenetwork.org/library/particular-threats-to-childrens-care-and-protection/covid-19/alternative-care-and-covid-19/guidelines-for-virtual-monitoring-of-children-their-families-and-residential-care-facilities-during