

OFFICIAL



**Australian Government**

**Department of Foreign Affairs and Trade**

# **DFAT CHILD PROTECTION GUIDANCE NOTE USE OF IMAGES AND SOCIAL MEDIA**

**May 2026**

**DFAT.GOV.AU**

# DFAT CHILD PROTECTION GUIDANCE NOTE USE OF IMAGES AND SOCIAL MEDIA

## Purpose

This Guidance Note offers guidance for **DFAT staff and partner organisations** on how to address the protection and wellbeing needs of children and young people when using social media, including when taking and using their images for program promotion within social media.

## Background

Civil society development organisations (CSOs) have quickly adopted the use of social media and new technologies, which they use to promote their development work; raise funds; advocate to and interact with donors, communities and potential supporters; and raise awareness of their programs.

Many programs provide children and young people with access to social media, often via organisation-hosted sites. Organisations must ensure their online environments are as safe as possible, and need to teach children and young people to be safe and responsible online users.

Children and young people also have access to and use social media and new technologies beyond your program. With increased social media use in the Asia–Pacific Region,<sup>1</sup> organisations must consider the broader risks to children and young people: how and why they access social media; and their attitudes to and understanding of online safety.

Children and young people in the Asia–Pacific region generally have a low understanding of online risks, such as grooming, bullying, financial frauds, and sharing personal and private details online. They may engage in risk-taking behaviour such as unsupervised communication with people online, or face-to-face meetings with ‘virtual friends’ (people met online) without knowing who they are.

In addition, organisations regularly use images of children to tell a story of need or program success. Organisations need to balance the benefits to the organisation and the risks to individual children, such as retribution, stigmatisation, or increased targeting by child-sex offenders including AI-generated Child Sexual Abuse Material.

Organisations must base all image gathering and publishing processes on ethical standards: assessment of risk to the child (with extra care taken for especially vulnerable children); child safety; respect of the child’s rights, integrity and dignity; obtaining and documenting informed consent from the child’s parent/caregiver and, if possible, the child themselves. Organisations must prioritise the best interests and protection of children over the opportunity for advocacy and promotion of the agency.

Please read this guidance note in conjunction with:

- DFAT’s Child Protection Policy (<http://dfat.gov.au/about-us/publications/Pages/child-protection-policy.aspx>)
- DFAT’s Establishing Child Protection Risk Context Guidance Note (<http://dfat.gov.au/about-us/publications/Documents/child-protection-risk-assessment-guidance.pdf>).

<sup>1</sup> *Internet Seen as Positive Influence on Education but Negative on Morality in Emerging and Developing Nations* Pew Research Center. March 19 2015. – <http://www.pewglobal.org/2015/03/19/internet-seen-as-positive-influence-on-education-but-negative-influence-on-morality-in-emerging-and-developing-nations/> The survey was conducted among 36,619 people in 32 emerging and developing countries during 2014. See <http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-apac-in-2015?related=1>

# RISKS IN USING SOCIAL MEDIA IN DEVELOPMENT PROGRAMMING

**Table 1: Risks of providing children and young people access to social media in development programming**

<b>RISK</b>
<b>1. Child or young person is abused or exploited when using organisation-hosted social media sites</b>
<b>2. Child or young person is abused or exploited when using social media sites external to the organisation</b>
Examples of this include: online grooming, sexual abuse or sexualised language or posting of inappropriate content, bullying and discrimination (verbal and physical bullying, threats, shaming, humiliating, teasing).

## Mitigation Strategies

### Research attitudes and behaviours

- Within their local context, research: how, where and why the children in programs do or are likely to access the internet/social media platforms; and their online attitudes and behaviours.

### Ensure that impacts on children are considered at the concept and design stage

- Undertake a child protection risk assessment of organisation-hosted social media sites and program designs, and monitor throughout the project cycle. Consult with children and young people as part of this process as they will identify different behaviours, attitudes and risks.
- It is crucial that, as with any other projects, the consideration of child protection risks is included in the overall risk assessment when developing or before adding content to social networking sites.
- Think about what the specific risks to boys and girls could be. Girls and boys use social media differently and are vulnerable to different risks.
- Consider the risks of children using skills learned in the agency program to go online beyond the program.
- Try to develop a project that influences online behaviour change in addition to providing general guidance on online safety.
- Be mindful that children and young people are likely to have access to the internet and social media platforms outside the program (via mobile phones, cyber cafes, school, home). Consider this when designing the project, resources and training.

### Ensure adequate policies and procedures are developed and implemented

- Develop a social media policy.

### Obtain informed consent

- Obtain informed consent from parents and children and young people for their participation in the project.

### Train staff and volunteers

- Train staff and volunteers in child protection and the risks to children using the internet and social media platforms, with a focus on gender, local, and cultural contexts.
- Investigate local legislation about the use of images, informed consent, and social media. Include this in training.
- Provide ongoing training and guidance to children and young people about online safety that is relevant to them and their cultural and social contexts. Include guidance on:
  - the dangers of sharing personal and private details
  - posting inappropriate content or images of themselves or others online or via mobile phones
  - online grooming behaviours
  - face-to-face meeting virtual friends.

### Implement safe systems

- All organisation-hosted social media sites should include child-friendly guidance on keeping safe online, including the expectations that children should expect from adults on the platform
- Investigate and use safe and closed (non-public) online forums to host social media sites, and forums with member only and password access.
- Make sure organisation-facilitated programs involving children accessing social networking are moderated by an adult trained in child protection.
- Ensure a trained staffed member screens all content before uploading.
- Work with children and young people to establish a project code of conduct and online user rules (including no personal or identifying details, using avatars, no geotagged images, or using a group identity).
- Ensure there is a reporting mechanism in place for child protection and safety concerns.

**Table 2: Risk in using images of children within social media**

RISK	
1.	Children or young person's rights to protection, privacy and dignity are infringed, and their vulnerability increased due to being pictured in undignified ways
2.	Images published on social media are misused or used in the production of child exploitation material, including AI-generated Child Sexual Abuse Material
3.	Children or young people are exploited and abused by photographer
4.	Child or young person is contacted or located by an offender because of disclosure of personal identity and location in a photo
5.	Child or young person suffers retribution and punishment due to disclosure of personal identity and location in a photo

## Mitigation Strategies

### Ensure adequate policies and procedures are developed and implemented

- Comply with DFAT's Child Protection Policy, including having a child protection code of conduct, which includes a section on appropriate use of images. Ensure staff understand and sign onto this.
- Develop and implement a policy or guidelines about the use of images. Include detailed information about obtaining informed consent.

### Ensure images of children are dignified and respectful

- Images of children should show them suitably dressed, to avoid them being misused or breaching the child's privacy and dignity.
- Do not use images of children in poses that could be interpreted as sexually suggestive. Consider how it may be viewed in different cultural contexts.
- Be culturally sensitive. Talk to field staff and communities to find out how they would like to be represented, and whether there are any cultural taboos or anything photographers and staff should avoid doing.
- Never use images of a child who has died or is in severe distress without any visible signs of help nearby.
- Consider watermarking images online to deter images being misused.

### Train staff and volunteers

- Train staff, volunteers, contractors and consultants in the organisation's child protection and use of images policies and procedures.
- Brief visitors to the field (consultants, donors, photographers, etc.) on taking images and use of images. Include rules about uploading images of children and personal information onto social media platforms. Make sure they sign onto the organisation's child protection policy and code of conduct.

### Obtain informed consent

- Develop and implement robust informed consent procedures that include:
  - Prior to taking photos, obtain informed consent. Informed consent means a parent/guardian and if possible, a child must understand and acknowledge what they are giving consent for. Explain (in local language) how the photograph, words or film will be used (where, how, for how long the image will be available for use by the organisation, whether it will be used on social media and internet sites where your organisation will not be able to control further use and distribution).
    - » Show examples of how images may be used.
  - Always gain informed consent from a child's parent or guardian and obtain the direct consent of the child or young person wherever possible. Ensure written consent forms are in local language.
    - » Oral consent is accepted but clearly document any oral consent and include it with the photo.
    - » All consent documentation should be stored in a secure location.
  - Explain and discuss the possible outcomes of using the images or giving an interview and publishing a story, particularly where there could be a negative impact on a child.
  - Explain that children and parents/caregivers can withdraw their consent at any time and provide them with a contact to do this. Advise that, because of the permanency of the internet, withdrawal of consent may not always lead to the removal of an image online.
  - Ensure the organisation has a process for removing images from the image library.
  - Allow time for the consent process to make sure that children and young people do not feel pressured to say yes to something they do not want to do, consider the possible power imbalance that may be present.
  - Always make sure children have a person of their choice with them and never be alone with a child.

- Make sure parents and children are prepared and briefed prior to taking images. This includes: informing them of what will happen; who will be present and where they are from; the purpose of the visit; what is acceptable and unacceptable behaviour; what they can do if they do not feel comfortable; and that they can stop at any time or say no to anything without any negative impact.

### **Undertake child-safe recruitment measures**

- Undertake child-safe recruitment of all organisational staff and volunteers. See also *DFAT Child Protection Guidance Note – Recruitment and Screening*.
- Ensure consultants and contractors also undergo child-safe recruitment processes and are supervised by staff when in contact with children.
- Ensure agreements and contracts with external consultants and suppliers include child protection clauses related to taking, use and storage of images. Images should remain the property of the agency, and photographers should be informed that they cannot be used for any other purpose, and/or that originals and any copies must be given to the agency or destroyed.
- Do not allow photographers to be unsupervised with children. Always accompany external photographers to field locations. Always allow the child to select who they want their chaperone to be (parent, teacher, agency staff, etc.).

### **Conceal identities and locations**

- Be mindful that showing children in vulnerable situations can make them targets for abuse and exploitation: images of children alone and isolated increase their vulnerability.
- Do not underestimate the reach of the internet. A picture of a child published on an Australian website can be viewed by someone in that child's community overseas. The internet is a huge and unregulated space, and this poses potential risks for the children organisations work for.
- Turn off the geotagging functions on still and video cameras and mobile phones.
- Conceal the identity of vulnerable and at-risk children. Do not show a vulnerable child's face or represent them in any way that may lead to their identification. This may mean changing names and locations or using district or country names instead of village names.
  - Where names and locations have been changed a disclaimer should be used, for example, 'The names and location have been changed for child protection and privacy purposes.'
- Identifying information should not be included in images and stories about children. Do not use the child's full name, or use their name with other personal information (such as village name, school name, street signs or names of family members) which may identify their location. If in the picture, these should be blurred out.
- Do not identify survivors of sexual exploitation, gender-based violence or abuse as such.
- An individual's status as a person living with HIV, TB or any other serious health conditions must not be revealed without written consent.
- Do not identify an individual's engagement in culturally unacceptable activities, for example, activities that include promotion of child rights or that challenge gender norms, engagement in sex work, or other socially marginalised or criminal activities.