Digital Safeguarding Guidance

Digital safeguarding contributes to how Amnesty International UK (AIUK) keeps safeguarding at the heart of our activities and aims to ensure that no one engaging with AIUK's work are put at risk through any online activities we provide. This guidance explains how to stay safe online.

At AIUK the use of online spaces, such as having virtual meetings, has increased. There are lots of benefits of interacting online including staying in contact with individuals outside of face-to-face meetings, activities and events and facilitating active participation of people in our human rights activities. But there are additional risks when using social media and other online forums to communicate with individuals, particularly those who are under 18.

As a result, this document aims to provide guidance and expectations on conduct required by staff, volunteers, activists, board members and other adults involved in facilitating online AIUK activities, advice on specific online activities and reporting procedure when suspected abuse has occurred or concerns are raised.

This guidance should be read alongside the AIUK Safeguarding Policy and Procedures.

What do we mean by digital safeguarding?

Digital safeguarding means doing all we can to protect everyone who engages with AIUK from online harm. These harms can include;

- Cyberstalking – Repeatedly using electronic communications to harass or frighten someone. For example, by sending threatening messages.
- Discrimination and abuse on the grounds of protected characteristics – It can be an offence to stir up hatred – 'inciting hatred' - on the grounds of any of the protected characteristics.
- Disinformation - Deliberate intent to spread wrong information.
- Doxing - the action or process of searching for and publishing private or identifying information about a particular individual on the internet, typically with malicious intent.
- Hacking – Accessing or using computer systems or networks without authorisation, often by exploiting weaknesses in security.
- Harmful online challenges – Online challenges sometimes show people doing dangerous things. People share these posts on social media, encouraging others to do the same.
- Hoaxes – A lie designed to seem truthful.
- Impersonation - Where someone pretends to be someone else online. This is often by taking photos from social media to build a fake profile. This is sometimes known as 'catfishing'.
- Misinformation - Where someone shares information they think is correct, but it isn't.
- Online bullying - Offensive, intimidating, malicious, insulting behaviour and abuse of power online. This can humiliate or denigrate people.
- Online harassment - Unwanted contact online intended to violate someone's dignity. It could be hostile, degrading, humiliating or offensive.
- Promotion of self-harm, suicide and eating disorders – Content encouraging these harmful behaviours on social media.

- Sexual exploitation and grooming online - Developing a relationship with a child with the intention of abusing them. Offenders use emotional and psychological tricks to build relationships. The abuse can take place online or offline.
- Sharing of illegal and inappropriate imagery - 'Illegal' means child sexual abuse imagery and imagery that incites violence, hate or terrorism. 'Inappropriate' could mean sharing pornography, or violent or hateful content.
- Oversharing personal information - This includes information that makes someone identifiable, like their names or phone number. It may also include identifying details based on someone's protected characteristics.

AIUK aims to prevent these things happening within AIUK settings, but when it does happen we want to respond appropriately.

If you think anyone is at risk of the above, you must report it in line with the safeguarding policy as you would with any other safeguarding concern.

We will seek to keep individuals safe by:

- Having clear and specific procedures for how to interact/engage with children online when representing/working for AIUK.
- Risk-assessing all our projects, initiatives, programmes, activities, services and campaigns to make sure digital safeguards are in place.
- Ensuring all staff, activists, board members and volunteers have undertaken the appropriate safeguarding training for their role and are provided with support and advice when involved in leading online activities to ensure they are run safely.
- Having clear procedures for reporting safeguarding concerns.
- Expecting individuals to follow the same safeguarding guidelines that apply offline, when they are interacting with children online.
- Ensuring personal information about all individuals who are involved in our organisation is held securely and shared only as appropriate.
- Ensuring that images of people are used only after their written permission has been obtained, and only for the purpose for which consent has been given.
- Providing support and advice for staff and volunteers and others involved in leading our activities online about online safety.

In this guidance we will look at…

Behaviour and conduct expected of organisers and staff/activists/volunteers/board members working virtually/online with groups.

Best Practice:

- Ensure wherever possible, there are two designated adults involved in any activity supporting activists under 18, such as online meetings etc. Please refer to the criminal record check policy to establish if these adults will need checks.
- In online groups for projects, such as WhatsApp or Facebook groups, best practice would be that all adults should have had criminal record checks. This is due to regular contact with activists under 18, the sharing of personal contact details and increased risk of grooming.
- In virtual meetings at least one adult present needs to be criminal record checked.
- Private messaging a child or young person on a work phone or work social media account such as WhatsApp, should be avoided where possible. It is better to post a message to the whole group in the presence of other staff members/adults or email individual activists under 18 on your work email address and copy in parents, particularly for children under 13. If you do need to direct message a young person, it should be one off and an on-going dialogue should be avoided. If this is needed for a specific project then it should be recognised as an additional risk in the risk assessment, the adult should be criminal record checked and parental consent should be gained first.
- Only ever use an organisational device to communicate with activists under 18, you should never initiate contact from a personal mobile. If this isn't possible, for any exceptional reason, this should be discussed with the safeguarding manager who along with line managers should

authorise individual staff and volunteers to use a personal device on a case-by-case basis and keep a record of this authorisation and outline which circumstances it should be used for within a risk assessment.

- Staff, lead activists and volunteers should never give activists under 18 under the age of 16 who they are working with their personal contact details or add, follow or interact with them using a personal social media account.
- Use an age-appropriate platform and follow the platform's community guidelines and terms and conditions. For example, WhatsApp's age limit is 16+ and therefore it should be discussed with the young person and their parents if this is an appropriate platform.
- Consent is required from parents of all under 18s, to engage in new online activities with AIUK, in the same way as it is set out in the safeguarding at f2f events guidance and they should be directed to this guidance. 13+ should also sign the consent form themselves before engaging.
- Use age-appropriate language when interacting online.
- Staff, activists, volunteers and board members, should also be aware of their own social media's and what is accessible to the public. People may look up the personal social media accounts of people who are working with them at AIUK, so it is advised that their accounts are private or be free of content which goes against AIUKs values/aims or is offensive. They should not provide any personal information such as address, personal email addresses or phone numbers.
- Consider the room you are in for video activities and what might be visible in the background. Make sure you and others on view are dressed appropriately.
- Value and take all participants, including activists under 18's contributions seriously, actively involving them in planning activities wherever possible.
- Respect a young person's right to personal privacy as far as possible, except where there are safeguarding concerns which put them at risk of harm.
- Treat all involved, fairly and without prejudice or discrimination.
- Understand that activists under 18 are individuals with individual needs.
- Respect differences in gender, sexual orientation, culture, race, ethnicity, disability and religious belief systems, and appreciate that all participants bring something valuable and different to the group.
- Challenge discrimination and prejudice.
- Encourage activists under 18 and adults to speak out about attitudes or behaviour that makes them uncomfortable.
- Promote relationships that are based on openness, honesty, trust, and respect.
- Avoid favouritism.
- Be patient.
- Exercise caution when you are discussing sensitive issues.
- Ensure your contact with activists under 18 is appropriate and relevant to the work of the project you are involved in.

When working virtually/online with groups, you should avoid:

- Allowing concerns or allegations to go unreported.
- Taking unnecessary risks.
- Smoking, consuming alcohol or using illegal substances during the meeting.
- Developing inappropriate relationships with activists under 18.
- Making inappropriate promises to activists under 18.

- Engaging in behaviour that is in any way abusive or harmful, including making sarcastic, derogatory or sexually suggestive comments or gestures to or in front of those engaging with the online activity.
- Acting in a way that can be perceived as threatening or intrusive.
- Sharing individuals personal details with others outside of the group.

Safeguarding considerations for different online activities

Online meetings, workshops and committees (closed groups)

- Always undertake a risk assessment during the planning stages of commencing new activities online, especially considering the risks when activists under 18 could be involved. Things that should be considered in the risk assessment include the medium you will be using, and understanding the risks associated with that medium. For more information about risk assessing online activities, the NSPCC has some guidance here. If you are worried about any safeguarding risks, consult with the AIUK safeguarding manager.
- Be mindful of different age restrictions for different mediums, you can see age limits here. It is advisable to discuss the medium and any mitigations with the safeguarding manager if you are unsure.
- In the risk assessment, it is also important to think about the content which will be covered in the sessions, and whether it is appropriate for activists under 18, taking account of any individual situations you might be aware of.
- For activities delivered regularly in a closed group involving activists under 18 (as opposed to one off or irregular activities), this may necessitate a criminal records check to be carried out on adults present, since they will have regular access to activists under 18. But this will depend on the medium used, and it may be sufficient to have minimum number of criminal record checked staff present depending on ratio of activists under 18, where the medium used does not enable adults to directly contact activists under 18 outside of the meetings. See the NSPCC guidance on adult: children ratios required. You can also check the AIUK Criminal Record Check policy and discuss with the safeguarding manager if you need further guidance.
- You should seek parental consent for new activities delivered online involving activists under 18 and direct parents/carers to this guidance. Within this consent the activists under 18 should also agree to adhere to the Activist Code of Conduct, which details expectations of behaviour and can be found here.

During the activities:

- For closed meetings, always ensure a system of registration is in place, so you know who is 'in' the virtual space. Another tip is to have a virtual waiting room before the meeting starts (if the medium provides this, such as Zoom) to ensure you can individually admit attendees you are aware of. Or an alternative, is password protected access, so only those sent the password in advance can be admitted to the meeting. If you are using Teams, it enables you to admit people out of your organisation.
- Before the main part of the meeting/activity commences, it is important as part of the introductory part to outline the importance of creating a safe space with activists under 18 attending, asking attendees not to record (or making people aware if it is being recorded) and making it clear that inappropriate behaviour will not be accepted and also making clear how activists under 18 (and other adults) can report behaviour which is inappropriate.
- If unacceptable behaviour is witnessed by a staff member/activity coordinator, it should immediately be addressed, ideally privately, but if that is not possible, they may need to be

asked to leave or the meeting stopped whilst the issue is resolved. For more information see relevant section below.

- If a young person or another adult reports an allegation of abuse or you are concerned about their welfare during the activity, these should be immediately acted upon in accordance with the reporting procedure.
- If you see something which you are worried about, always get in touch with the individual after the activity, to check in that they are ok. If it is a young person, do this with another adult present.

Public events and livestreaming

Livestreaming can be used to broadcast events or activities in real time, from anywhere and at any time. Some livestreams can also be saved and kept on social media platforms to view later. In organising a livestream public event it is therefore important to recognise there is always a chance that activists under 18 may be present, even if the event is not expressly targeted at them and you should always assume that a young person could be attending a live public event and plan as such for this possibility. The following steps should be taken:

- Always include safeguarding in the risk assessment at the planning stage for new livestream events. In the risk assessment think about factors such as the content being covered during the activity and whether it is suitable for activists under 18 - if it includes particularly sensitive content, it may be preferable to use an application which participants must register in advance for, requiring age to be disclosed and parental consent.
- Since it will not always be practical or possible to obtain parental consent for all live open public events, in situations where it is not possible, you will instead need to put up a content warning in a prominent place, depending on the nature of materials covered. For material where there is some risk of material not suitable for younger teens, such as bad language/references to sensitive human rights abuses/sexual content you will probably state that content is only suitable for young people aged 16+ or accompanied by a parent.
- At the planning stage, think about staffing and if there is a live chat, ensure a member of staff will be fully focused on moderating content during the event to remove abusive or inappropriate messages instantly.

If it is a live two-way participative closed event, (as opposed to an open event with speakers mainly doing the talking), there will be slightly greater risks and the following should be borne in mind:

- Consider how to make sure your livestream only includes the people you've invited. For example, you might be able to ask your audience to register to watch the stream and issue a log in and password. Or you could look into using a custom platform if you regularly livestream.
- If possible, ensure the platform you're using is accessible to Deaf and disabled individuals. For example, you could use screen readers, subtitling or transcripts if using Teams.
- Whoever is appearing in the livestream, should make sure their surroundings and environment are appropriate.

Points to highlight to activists under 18 before a closed live event commences:

- Even if a participating child can't be seen in your stream there may still be identifying information such as their name, email address or a link to their social media account.

Encourage all people (therefore including activists under 18) to log in only with a first name and not reveal the full identity of individual participants.
- Live streaming is live, in real time. It should be highlighted before the activity commences that any comments made will be seen by others, and they may not be able to delete or edit what's been said.
- Children shouldn't share any personal information during a livestream. Remind all individuals in a disclaimer at the beginning what personal information is and not to respond to contact requests from people they don't know.
- Some livestreams request donations from the audience. Explain to everyone that they don't have to contribute.
- Make sure that all present know who to tell if they see or hear anything upsetting or inappropriate.

Local group meetings

For local Amnesty groups which have their group meetings taking place online, there will need to be safeguards put in place to ensure activists under 18 attending are safe:
- A risk assessment should always be carried out by the branch chair or other member of the local group leadership structure. This will consider factors such as the medium to be used for local group meetings, thinking about measures to minimise risk (such as using first names as opposed to full names when logging in) and ensuring a registration system, so you know everyone who is attending and ensuring invites/entry is password protected to participate in the online meeting.
- If it is a regular online meeting, you should seek parental consent for under 18s to attend and make them aware of the nature of the meetings taking place online. If you have consent for the young person to attend face-to-face meetings, it is important to make sure the parent/carer is aware of the online meeting, but separate consent should not be needed. Within this consent the activists under 18 should also agree to adhere to the Activist Code of Conduct, which details expectations of behaviour and can be found here. If a young person is attending with their parent, parental consent is not needed.
- Ensure that the introductory part of meetings highlight that there are activists under 18 present and the need to ensure no offensive or abusive comments, and also make it clear how activists under 18 can report any concerns (either by direct message to the hosts in the meeting itself or through a separate phone conversation/email).
- If any concerns are reported, do not ignore them. Report concerns to the AIUK safeguarding manager in accordance with the reporting procedure or if you are unsure about a concern.
- If there has been any offensive behaviour which has been addressed in the meeting, also follow up with the individual harmed and any bystanders after the meeting, to make sure they are ok.

Online closed communities (such as Facebook groups, or WhatsApp groups)

Communities can be hosted on a semi-permanent/long term basis on online forums or social media groups. Different platforms and apps enable different benefits, but these platforms also pose significant risks since they can give adults access to either a young person's private phone number or social media profile, which could potentially facilitate grooming activities. As a result, the following should happen.

- Planning and risk assessments should be carried out when seeking to use mediums and processes which minimise risks of opportunities for abuse to take place. This includes using mediums which do not give personal details such as phone numbers or full names of activists under 18. If this is not possible, all adults in the group either staff or committee members/activists should be criminal record checked since they will have regular contact with activists under 18.
- At the start of any project, group or event which includes use of closed online communities, consent should be obtained from parents/guardians for all activists under 18 who are part of the group and this should include the consent from both the young person and parent/guardian to be part of the group. If consent is not given, alternative ways to communicate information with the young person needs to be considered, to be inclusive.
- It should be made clear to all involved how they can report anything upsetting or inappropriate and make clear who they should report to.
- To make sure children are not exposed to harmful or inappropriate content you will need to moderate your community. This means checking and reviewing what people are posting to assess whether content is appropriate for activists under 18.
- As previously highlighted, you should not be private messaging activists under 18 outside of the group. It should be made clear to activists under 18 before joining the group that staff/adults are not allowed to do this, and if a young person attempts to send private messages you should respond to the group. Where there are safeguarding concerns raised by the young person or they have reached out for support this would be different, but it would still be advisable to follow up contact with another adult and explain to the young person why. If a one-to-one follow up is required, as a last resort you should telephone them to speak about the matter, making a record of the conversation and then report the concerns to the safeguarding manager and agree on a course of action.

Challenging inappropriate behaviour online/ responding to online abuse

During a meeting:

- If inappropriate behaviour occurs during a meeting, activity, or workshop, this should immediately be challenged and stopped by the event/activity organiser. Ideally this should be addressed privately if possible. If the person instigating the behaviour continues, you should repeat that this is unacceptable a second time. If the person still continues, then at this point for the safety and wellbeing of others present, the person should be removed from the group, or if this is not possible depending on the online medium, the entire activity should be stopped and the activity organiser should explain that this is because AIUK cannot facilitate activities which are abusive or threatening.
- If a young person is making the abusive or threatening remarks, particular sensitivity should be observed in calling out the conduct of the young person in front of peers. Often the easiest way to do this, is to discreetly say that it is time for a 5-minute comfort break, and during the break the young person should be contacted, ideally by two adults, to explain what has happened is not appropriate and to discuss the matter before the activity resumes.
- In all cases, where abusive or threatening behaviour has occurred with activists under 18 present, if possible, the activity organiser should contact all activists under 18 in attendance afterwards to check that they are okay. For online streaming activities, there is a separate procedure since we won't always know who has attended (see section on livestreaming and public events above).

- In accordance with the reporting procedure, all instances of inappropriate or abusive behaviour should **always** be reported to the safeguarding manager, who will discuss any further action needed or follow ups with the person who instigated the inappropriate behaviour and so that it can be recorded centrally in the safeguarding risk register.

Social media harassment:

- The work done by AIUK is public and regularly receives media attention, including responses on social media which may be negative and could include harassment of individuals involved with AIUK's work. Whilst we are unable to prevent this harm, the risk can be minimised by risk assessments being done for projects which include this risk and considerations being made to how it can be managed, for example ensuring those involved with AIUK and that specific project, have good privacy settings in place on their social media accounts.
- For activists under 18 who are lead activists, when they take on this role, discussions should be had with them about this risk, and how to respond to it and protect themselves. They should be encouraged to make their social media private and advised to report any harassment as soon as it occurs to other lead activists and the safeguarding manager.
- If harassment, such as doxing or trolling, is occurring, it should not be ignored, and you should not feel you have to manage it alone. In the first instance reach out to your manager and/or colleagues (if appropriate) for support, you can also reach out to the safeguarding manager.
- For more information on how to respond you can look at the charity Glitch who give advice on what to do if you are experiencing online abuse www.glitchcharity.co.uk/resources/

Procedure for reporting concerns

If anyone, comes to a AIUK staff member, activist, volunteer or board member with a disclosure of abuse or there is any suspicion that abuse has or may take place, the individual should take immediate action. If it is an emergency they need to contact the relevant emergency services and follow up as they advice, then reporting the incident within 24 hours to the safeguarding manager who is the organisations Designated Safeguarding Lead. If there is no immediate risk of harm the concern should be reported to the safeguarding manager within 24 hours, who will follow up as needed.

Any inappropriate behaviour observed by staff, volunteers, lead activists, board members or others during online activities, should be dealt with and challenged within the meeting appropriately, and always reported to the safeguarding manager.

Safeguarding Lead Contact

Designated Safeguarding Lead (DSL):	Safeguarding Manager
Contact Details:	safeguarding@amnesty.org.uk

In many instances, it will be the case that the event/activity organiser will primarily deal with the safeguarding incident, after receiving advice from the safeguarding manager. However, it is imperative that all incidents are discussed with the safeguarding manager and recorded centrally in the Amnesty UK Safeguarding Risk Register if needed.

In relation to cases of abuse involving organisations who receive grants from AIUK, including DFID funded programs, they should report such incidences to an equivalent DSL locally, and thereafter

AIUK should be made aware of the disclosure without excessive delay.

Guidance on what constitutes abuse is set out in the AIUK safeguarding policy and more information provided in the Care Act 2014 and advice specific to defining abuse involving children is available from the NSPCC.

As far as possible, confidentiality will be fully respected, but the welfare of any adult-at-risk or child/young person is paramount and may necessitate sharing of information in relation to possible cases of abuse, neglect or where someone is at risk of harming themselves or others. In particular, the law requires, in certain instances the disclosure of the information to the appropriate body which may include a children's social care referral to the local authority where a young person is at risk, emergency services including the Police where a possible crime may have been committed or other statutory services in order to protect the person at risk and who may need critical support.

In all such cases, AIUK will endeavour to seek the consent of the person affected before making disclosures unless it is in their best interests not to do so.

Additionally, certain disclosures may also need to be made to AIUK Section and AIUK Charitable Trust boards and regulatory authorities such as the Charity Commission as required, where potential/ suspected breaches of our obligations have occurred. When suspicions involve adults who are in a position of trust with activists under 18 disclosures may be made to the Local Authority Designated Officer (LADO) or equivalent, for investigation as required under law. Disclosures are made to other agencies, in accordance with the relevant statutory guidance, in accordance with the requirements of GDPR legislation.

Alternative reporting mechanisms for activists under 18

In addition, to the formal AIUK reporting procedure, those participating in AIUK projects can also be made aware of alternative reporting mechanisms for online abuse:

- CEOP – CEOP is a law enforcement agency which works to keep activists under 18 safe from sexual abuse and grooming online. Activists under 18 can make an online report to CEOP (**www.ceop.police.uk**) if they are worried about something that happened when talking to someone online (this could be another young person or an adult): for example sexually explicit chat, asking for images, pressuring them, or threatening to share nudes. The young person will get help and support from a specialist child protection advisor.

- Childline – If a young person is nervous about speaking to an adult they know, they can always speak to someone at **Childline**. Childline can be contacted via a call or online chat confidentially, about anything: 0800 1111 or www.childline.org.uk. Childline run a service called 'Report Remove'. If a nude image or video of a young person has been shared online, the young person can report it to Childline, and they will work to have it removed from the internet.

Support/information:

- Internet matters – gives advice and guidance on different platforms and the risk associated with them - https://www.internetmatters.org/resources

- GLITCH - an award-winning UK charity ending online abuse and championing digital citizenship. They have a particular focus on Black women and marginalised people - https://glitchcharity.co.uk/
- The National Bullying helpline - provides information and advice for victims of online bullying or harassment - https://www.nationalbullyinghelpline.co.uk/cyberbullying.html
- NSPCC – For more information on the types of abuse, the effects and how to respond - https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/online-abuse/
- CEOP – For information on ways to report online sexual abuse https://www.ceop.police.uk/Safety-Centre/
- **Revenge Porn Helpline -** supporting support, advice and information to adult victims of intimate image abuse. Telephone 0345 6000 459 Tuesday – Friday 10am-4pm. - https://revengepornhelpline.org.uk/
- Speak Up & Stay Safe(r): A Guide to Protecting Yourself From Online Harassment - A Guide to Protecting Yourself From Online Harassment. - https://onlinesafety.feministfrequency.com/en/
- Get Safe Online – information about online safety - https://www.getsafeonline.org/