Girls' Education Challenge

Keeping in contact with girls

COVID-19 Communication and Safeguarding Guidance[1]

[1] Developed by Danielle Cornish-Spencer, Social Development Direct, on behalf of the Girls' Education Challenge, April 2020

Contents

Introduction

The Girls' Education Challenge (GEC) was launched by the UK's Department for International Development in 2012 as a 12-year commitment to reach the most marginalised girls in the world and is the largest global fund dedicated to girls' education. The UK is committed to ensuring millions of girls in some of the poorest countries, including girls who have disabilities or are at risk of being left behind, receive a quality education. Through the GEC, we aim to transform the lives of over one million of the world's most marginalised girls through quality education and learning. Access to a good quality education and learning opportunities will empower these girls to secure a better future for themselves, their families and their communities.

On 11 March 2020, The World Health Organisation classified the spread of COVID-19 as a pandemic. Currently, the worst affected locations are in North America, Europe and China, but the virus has started to spread in other locations. The GEC operates in 17 countries.[2] Of these 17 countries, at the time of writing, all have closed schools. Although guidance and action to stop the spread of the virus varies from county to country, mass gatherings are prohibited, and many contexts have asked people to stay at home – impacting on economies at the macro and micro-levels. It should be noted that even if cases have not been officially declared in some of the countries of operation, the quality of health care and the strength of health systems in many of the contexts in which we work may mean that there *are* cases, but that there are limited resources to diagnose and treat.

Box 1: Access and control of resources and do no harm

The Girls' Education Challenge, works with adolescent girls and young women. In thinking through ways in which we may safely keep in contact with girls, we also need to consider girls' access and control of resources. Projects should ask the following questions of their proposed ways of keeping in contact:

- Will girls have access to this technology already?
- What kind of access do they have (independent or through a parent/caregiver)?
- If we introduce a new piece of technology into the home, will the girl be able to access and control this technology?
- If we introduce a new piece of technology into the home, will this increase the likelihood of intimate partner violence, or family violence?

The importance of keeping in contact with girls safely

In light of the impact of Covid-19 on GEC project activities, projects should use 'reasonable endeavours' to remain in contact with beneficiaries, if safe to do so. Projects should draw on their existing safeguarding, ICT and data management policies to try to ensure appropriate safeguards are in place whilst keeping in contact.

Keeping in contact with beneficiaries is important for a number of reasons, including:

- ensuring that your project can support girls to continue to access education through distance learning initiatives or when in-person learning resumes
- ensuring girls do not drop out of educational activities during the COVID-19 crisis
- checking in on girls' well-being, so that referrals can be made, or projects can adapt to girls' needs.

Keeping in contact with girls in some way is a priority for GEC projects. Many of our projects have proposed a wide variety of methods to keep in touch and use distance learning that involve communications. These differ from project to project and context to context.

This guidance outlines ways that GEC projects should engage in communication methods from a safeguarding perspective. This is informed by traditional child safeguarding and protection from sexual exploitation and abuse perspectives, and incorporates elements of do no harm as well as questions for projects to think through regarding COVID-19. We primarily focus on interactive methods of communication

[2] Afghanistan, DR Congo, Ethiopia, Ghana, Kenya, Malawi, Mozambique, Nepal, Nigeria, Pakistan, Rwanda, Sierra Leone, Somalia, Tanzania, Uganda, Zambia, Zimbabwe.

(where communications are bi/multi-directional). Further tools regarding IEC materials and broadcasting will be sent to projects separately.

This document should be used as a supplement of our GEC Safeguarding Guidance Note.[3] Importantly, projects must ensure that: (1) their service mapping; (2) referral pathways; and (3) safeguarding reporting mechanisms are updated and communicated **as a priority.** The actions outlined below cannot take place without these three foundational pieces of safeguarding work in place.

Before implementing any activity, as practitioners we must first ask ourselves whether it is ethical and safe to do so. This involves asking ourselves a number of questions:

- Have you asked girls and their parents if they want to keep in contact and how they would prefer to do this? Are you offering a number of ways to keep in contact? What could be safe and accessible for girls today, may change tomorrow.
- What is the motivation? Is it to share resources? Is it to share education materials? Is it to check on the welfare of girls? Having a clear objective for 'why' the project wants to keep in contact will enable you to use the most appropriate communication method.
- How are local actors working on this issue already? Is that safe? Could we use this system rather than creating a new one?
- Who does the methodology benefit and who could be placed at risk?
- Do we feel confident that the benefits for girls outweigh the risks?
- Are we generating expectations or demand that the project cannot meet and could this lead to apathy or harm?
- Have we thought through the unintended consequences of embarking on this project?
- What will happen when the schools and projects return to their usual ways of working? Will communication mechanisms set up specifically for COVID-19 continue? What could be the harm of withdrawing these communication methods?

A note on grooming and sexual exploitation and abuse (SEA)

The risk of grooming is particularly acute within the context of the COVID-19 lockdown, in addition to other forms of sexual exploitation and abuse. Grooming refers to: *a process of socialisation through which an adult engages with and manipulates a child or young person for the purpose of sexual abuse (which may include online and offline aspects).* All of the methods to keep in contact described below, in the context of COVID-19 in particular, have a heightened risk of grooming and SEA taking place. Whichever form of keeping in contact or communication is used by a project, a number of actions should be taken to mitigate the risk of grooming and abuse. A non-exhaustive list of mitigation measures is provided below, and this may be added to by projects according to the type of communication they are using and their context.

Basic mitigation measures

- Promote behaviour protocols to girls engaged and adapt these behaviour protocols to your communication methods if needed
- Re-share and/or re-train staff in your existing code of conduct and adapt codes of conduct to communication methods used if needed
- Promote reporting pathways using your new communication method as a means to share
- Do not share staff members' personal numbers
- Ensure facilitators are female wherever possible. Although women can perpetrate safeguarding incidents, they are far less likely to sexually abuse adolescent girls
- Ensure staff and those facilitating communication do not contact girls outside of pre-agreed times that are logged in a communications log-book (maintaining confidentiality if discussing safeguarding, protection or other sensitive issues).

[3] See: https://dfid-gec-api.s3.amazonaws.com/production/assets/34/Safeguarding_and_COVID-19_Partner_Guidance_April_2020.pdf

Keeping in contact: using phones

Using phone calls and SMS to keep in contact with girls in the current context of COVID-19 is both a logical and a popular methodology proposed by many of our partners. It is important to keep in mind, however, that although the level of in-person exposure is limited, there are still risks involved in keeping in contact through the phone and the GEC consider this kind of contact as a major risk.

Texting/SMS can be a good means of reaching girls. The technology is widespread and not limited by whether girls have a smart phone or an older phone as all mobile phones have a default texting function. However, projects should consider access and control (see box 1) of telephones and whether these are a viable means of communication in their context. Where appropriate, projects may want to consider using SMS as a broadcast from a work computer with girls responding with 'yes/no' to questions, rather than working through mobile phones and engaging in full SMS conversations with girls. Tis is likely one of the safer options for keeping in contact with girls and mitigates the risks of abuse.

Safeguarding considerations

- Has the project thought through the safety and well-being of staff members and their work-life balance? For example, does the use of the new communication method mean that staff will be 'on call' at all times, or will there be a plan put in place for handover, call forwarding and/or operating hours?
- Will devices be 'work' or 'project' devices? If using project-owned devices, the project will then be able to better manage data security with the phone network provider and on the phones themselves – deleting messages, call logs or deleting information on the whole device (if internet enabled) if the device is stolen. The risks involved in using a personal device include: friends and family could see girls' personal information, the staff member may have to hand over their personal device in police investigations regarding safeguarding complaints, or staff members may not be able to 'switch off'.
- Projects should always ensure they are adhering to data protection laws, confidentiality and that personal data is not stored without informed consent. All projects should already have data protection policies in place. Projects should refresh their knowledge of their own policies. In addition, see Annex 1 for tips on privacy and safety.
- When working through the phone with girls and vulnerable adults, projects should adhere to the same safeguarding policies and procedures which would apply in person. All projects should have a suite of safeguarding policies and procedures, codes of conduct and behaviour protocols. These should be adapted, to specifically relate to using the phone.
- If communicating using messages in two-way communication, rather than via a broadcast methodology, it is important to remember that traces of these messages will be left on girls' phones. Girls may not have full control of their phone, and so messages may be read by others. See Annex 2. Tips for keeping phones safe for girls.

Projects must put in place a protocol for the way they will keep in contact using phones. The protocol must answer the questions or satisfy the considerations above. Projects should factor in budget to be able to deliver safeguarding components of their work.

Box 2. Helping girls say safe – 'sexting'

Where projects are actively encouraging girls to use phones to communicate, they have a responsibility to ensure that girls understand the risks involved. One of those risks is 'sexting' or sending nudes. This is when someone shares a sexual message, naked or semi-naked image, video or text message with another person. It doesn't have to be a nude image of them and could be an image of someone else.

There are lots of reasons why children and young people may want to send sexual messages or naked or semi-naked images or videos to someone.

These include:

- Peer pressure
- Being blackmailed, harassed or threatened
- To increase their self-esteem
- To prove their sexual orientation
- Being worried about not being seen as attractive, or as 'shy'
- Feeling like they 'owe' their boyfriend/girlfriend and being made to feel guilty if they do not
- Being in love with someone and fully trusting them
- They are in a long-distance or online relationship and want to have a sexual relationship.

Make girls aware:

Communicating to girls about the dangers of sexting and of sharing sexualised images of themselves is important, particularly as social isolation will mean that girls are more likely to engage through social media and phones (where accessible).

Risks include:

- Losing control of the images, videos or messages and how they are shared. Once something is shared online it is public and can be saved or copied by others.
- Blackmail, bullying and harm. Young people can have their photos, messages or videos shared without their consent or be bullied about them. This can lead to them feeling difficult emotions like distress or embarrassment and shame.

If projects receive reports of a safeguarding incident involving sexting, follow the normal reporting pathways withing organisations and to the GEC. Additionally:

- Staff and investigators must never view, download or share the imagery themselves, or ask a girl to share or download **– this would then become a separate safeguarding incident**.
- If staff have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), this should be reported to the safeguarding officer.
- **Do not** delete the imagery or ask the girl to delete it.
- **Do not** ask the girl(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the safeguarding officer only.
- **Do not** share information about the incident to other members of staff, the girls(s) it involved or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain to them that you need to report it and reassure them that they will receive support and help from the Safeguarding Officer.

Keeping in contact: in person

Keeping in contact in person, in the context of COVID-19, is even higher-risk than in times not affected by crisis. However, there may be a need (where all other methods are not suitable) to keep in contact with girls in person. For example, if a girl is known to be at risk of gender-based violence and does not have access to a phone, the project may choose to work with girls on an in-person basis to conduct basic welfare checks. The GEC notes that there is a shadow pandemic of violence against women and girls currently taking place along-side COVID-19, with increases in violence against women and girls, including murder, across all affected contexts. Similarly, where projects are working with girls with disabilities, welfare checks may be necessary during lockdown – where possible and where Personal Protective Equipment is in place to mitigate risk of spreading the virus.

Box 3: Personalising risk, mitigation vs. shifting risk, and staff/volunteer consent

With all of the methods to keep in contact discussed in this guidance note, it is important to consider if the project designer themselves would be happy to deliver this action, or to have their own child take part in this activity. In asking this question, we allow ourselves to explore if the proposed intervention is a shifting of risk (rather than a mitigation of it) on to volunteers or members of staff who have less power than those making decisions regarding the interventions to be implemented. Further, projects should ask their own staff and volunteers whether they are comfortable with the risks involved in delivering the proposed intervention at this time. Staff members and volunteers should be able to provide informed consent, without undue pressure to deliver project activities.

Keeping in contact in person, however, presents a number of risks projects need to consider and to mitigate. Below are questions for projects to consider in the design of their interventions in this area, to interrogate the risks involved in this intervention and ways to mitigate those risks.

Safeguarding considerations

- Has the project thought through other options? Is this the only way to keep in contact with girls?
- Do the risks to girls if left without contact (e.g. risk of GBV) outweigh other risks?
- Are all staff members and volunteers women? Is it safe for them to work on their own in that community (e.g. will you put in place regular check-in calls, could they work in pairs)?
- How would this be implemented in a way that does not identify the girls as 'at risk' or as survivors in their communities? Could well-being checks be conducted in a safe location away from the home (an information point, a water point or a distribution for example) where the sole purpose of engaging with people is not only protection focused?
- How will you ensure you are mitigating the risk of exacerbating intimate partner violence or family violence through visits?
- Are staff or volunteers already trained appropriately? If not, how can you train them safely in the current context?
- Do staff or volunteers increasing the time spent with girls have the appropriate background checks already in place?
- How will you monitor these visits? Could you implement a phone call monitoring system – of monitors and girls themselves?

Additional COVID-19 considerations

- In-person contact should only be conducted by staff/volunteers from the same community as girls. Travel to and from different communities presents too great a risk of spreading the virus.
- What personal protective equipment can you offer your staff members?
- How will you implement social distancing measures and ensure these are upheld?

In-person contact during this crisis, again, is very high risk. **Projects must put in place a protocol for the way they will keep in contact in person. The protocol must answer the questions or satisfy the**

considerations above. Projects should factor in budget to be able to deliver safeguarding components of their work.

Keeping in contact: 'group chats' and other online communications

Many of our projects have suggested the development of online communication, either for keeping in contact or for education purposes. There are a wide range of apps, tools and software to choose from. Again, however, projects must consider access and control (box 1) of resources and ensuring their approaches are girl-centred. Because technology has made something possible, it does not mean that this is the right modality to use for the girls we serve.

Creating an app or other online tool

Identifying and assessing data processing risks

Before setting up online communication, the risks to girls with regards to data processing must be considered. The potential impact on girls and any harm or damage your data processing may cause, whether physical, emotional, developmental or material should be thought through. You should also specifically look at whether the processing could cause, permit or contribute to the risk of:

- physical harm
- online grooming or other sexual exploitation
- social anxiety, self-esteem issues, bullying or peer pressure
- access to harmful or inappropriate content
- misinformation or undue restriction on information
- encouraging excessive risk-taking or unhealthy behaviour
- loss of autonomy or rights (including control over data)
- compulsive use or attention deficit disorders
- excessive screen time
- interrupted or inadequate sleep patterns
- economic exploitation or unfair commercial pressure
- any other significant economic, social or developmental disadvantage.

Box 4. Codes for safe reporting

Girls may not be able to report protection concerns or safeguarding incidents easily during lockdown due to a lack of confidentiality and privacy, lack of access and control of phones (or even where they are able to access phones, they may not be able to send a message without this being reviewed by family or partners).

Codes may be able to be developed by projects. These should be tailored to context. For example, where a girl speaks to a staff members or associated personnel on a phone and asks for "Mrs. Abet" to help with her homework, this signifies that she needs urgent help. Other codes could be communicated on the phone to girls, verbally to ensure that they are aware of the codes and that only girls are aware.

Lastly, there is a risk of impersonation across text-based platforms used to report (SMS, online chat and email). It is important that a code word or phrase is used with the girl to verify if it is her talking to you or whether they are being impersonated in order to access information which may put them at risk.

Finally, projects should make it easy for girls to be able to report problem content and to make a complaint about content or behaviour online which makes them feel uneasy. This may be through a standardised function for girls to report within the app/website itself.

Parental controls

Parental controls are tools which allow parents or carers to place limits on a child's online activity and thereby mitigate the risks that the child might be exposed to. They include things such as setting time limits or bedtimes, restricting internet access to pre-approved sites only, and restricting in-app purchases. They can also be used to monitor a child's online activity or to track their physical location.

They are important because they can be used to support parents in protecting and promoting the best interests of their child. However, they also impact on the girl's right to privacy and on their rights to

association, play, access to information and freedom of expression. Girls who are subject to persistent parental monitoring may have a diminished sense of their own private space which may affect the development of their sense of their own identity. This is particularly the case as the girl matures and their expectation of privacy increases. Projects must balance risk mitigation and the right to privacy carefully, particularly as projects primarily work with adolescent girls. Projects must make it clear to the child if parental controls are in place and if they are being tracked or monitored.

If your online service allows parental monitoring or tracking of a child, you should provide age appropriate resources to explain the service to the child so that they are aware that their activity is being monitored by their parents or their location tracked. You should provide a clear and obvious sign for the child (such as a lit-up icon) which lets them know when monitoring or tracking is active.

You should also provide parents with information about the child's right to privacy under the UNCRC.

Social media

Use of Twitter, Facebook, Instagram and other social media apps that require connecting via personal accounts are not at an acceptable level of risk for the GEC and projects should not keep in contact with girls in this way.

Existing video and chat tools

Here are a wide variety of video and chat tools available. Each one would need to be researched, with safeguarding considerations taken into account. The website, NetAware[4] provides information on the safety of many different apps and platforms. Projects should also consider whether or not the app is compliant with confidentiality laws in the country of operation.

Safeguarding considerations

- Does the tool collect and store personal data?
- Could the tool could be hacked? This is a particular risk where there is a link used to join and anyone with a link can join. With a screen sharing function, a hacker could share inappropriate materials or disrupt the call. This could be mitigated by limiting screen sharing privileges at the start of the call and asking girls not to share information on joining the call with anyone outside of the project.
- Can meetings can be recorded? Projects should talk to children before recording takes place and gain permission from parents. If recording, at the beginning of the call, the facilitator must remind them not to share personal information, like their name and phone number, or private parts of their body.

WhatsApp and similar communication tools

WhatsApp is an instant messaging app which lets you send messages, images and videos in one-to-one and groups chats with your contacts. Many of our projects are considering using this app. The GEC notes there are other, similar platforms available and that partners should explore the pros and cons of each before going ahead. Again, access and control must be factored into this decision.

Additional safeguarding considerations (the same considerations as above apply to these types of apps)

- Group chat can be used to bully
- People can get hold of numbers and, outside of group messages, send inappropriate content
- Projects could use 'broadcast function' instead of two-way communications but numbers are still visible
- At least two adult administrators should be on the chat at any one time

If considering the use of video and chat tools, consider these five points:

1. Is there an alternative way to maintain contact with the girls?
2. How will you inform parents and ensure they understand and agree to their daughters' participation (ideally, parents should understand the platform and how it will be used)?
3. Is there any way for parents to be part of the group (this may not work if the parents are the source of concerns, where parents' presence is a breach of the girls' right to privacy etc.)?

[4] See: https://www.net-aware.org.uk/

4. Who will moderate the platform on behalf of the project to deal with issues of misuse?
5. Clear boundaries should be articulated and understood by all users. Can the project team manage this?

Box 5: Survivors and technology

One in three women and girls will experience physical and/or sexual violence within their lifetime, most likely at the hands of an intimate partner. We know that violence against women and girls is going to increase during this crisis and many of the girls we work with will be quarantined with abusive partners. Technology is one way that violent partners or family members may control girls. According to one study, almost half of survivor of intimate partner violence said they were monitored online or with technology, through trackers, apps or internet blockers.

Given the potential for abuse, technology should be developed with safety as its primary goal. Technology dealing with sensitive subject matter should include the option for a 'quick escape' where the programme can be closed instantly and can be hidden. Apps developed for education purposes should also provide information on GBV and Child Protection services locally and nationally and share tips on how to stay safe.

If your project plans to use any social media, or mass communication app, please consult NetAware. This site will give you information about the risks involved. Projects should respond to and mitigate against those risks in their procedures. Projects must put in place a protocol for the way they keep in contact using web-based tools. The protocol must answer the questions or satisfy the considerations above. Projects should factor in budget to be able to deliver safeguarding components of their work.

Source material and resources

Chayn, 2020. Securing A Mobile Phone Or A Tablet: https://chayn.gitbook.io/advanced-diy-privacy-for-every-woman/securing-a-mobile-phone-or-a-tablet

Data protection laws of the world: https://www.dlapiperdataprotection.com/#handbook/world-map-section

Girl Effect, 2018. Digital Safeguarding Tips And Guidance: https://prd-girleffect-corp.s3.amazonaws.com/documents/Digital_Safeguarding_-_FINAL.pdf?AWSAccessKeyId=AKIAIWVYO5R6RMTXA2NA&Signature=9uRyrXXcikvwAYR9M1DivZniJ2w%3D&Expires=1586867812

Girl Effect, 2018. Digital Safeguarding Tips And Guidance https://prd-girleffect-corp.s3.amazonaws.com/documents/Digital_Safeguarding_-_FINAL.pdf?AWSAccessKeyId=AKIAIWVYO5R6RMTXA2NA&Signature=9uRyrXXcikvwAYR9M1DivZniJ2w%3D&Expires=1586867812

GOV.UK. 2020. UK Council For Child Internet Safety (UKCCIS): https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis#ukccis-publications

Information Commissioner's Office – The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/15-online-tools/

Livingstone, S., Davidson, J. and Bryce, J., 2017. Children's Online Activities, Risks And Safety. UK Council for Child Internet Safety: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759005/Literature_Review_Final_October_2017.pdf

National Network to End Domestic Violence, 2020. Safety Net Project: https://aoir.org/reports/ethics3.pdf

NetAware: website explores the safety of most popular apps: https://www.net-aware.org.uk/networks/whatsapp/

Snook, Chayn and SafeLives, 2017. Tech Vs. Abuse: https://safelives.org.uk/sites/default/files/resources/Tech%20vs%20abuse%20report.pdf

WhatsApp Coronavirus Information Hub for Educators: https://www.whatsapp.com/coronavirus/educator/

UK Council for Child Internet Safety. Child Safety Online: A Practical Guide For Providers Of Social Media And Interactive Services. UK Council for Child Internet Safety: https://www.gov.uk/government/publications/child-safety-online-a-practical-guide-for-providers-of-social-media-and-interactive-services

Annex 1: Tips on privacy and safety on platforms and products

**For additional information regarding specific points below, and tools and resources to support you, please see the source material.*[5]

Minimise the amount of data collected

- Only collect the data that is strictly necessary for legitimate business purposes such as:
    - Providing, operating or maintaining a site or application
    - Meeting an identified business purpose that the user is informed about (this can include research, monitoring and evaluation to improve content or measure impact)
    - Meeting legal obligations
- Only use data for purposes that users would expect, based on the information provided when they sign up or join, e.g. through Terms and Conditions and a Privacy statement.

Develop privacy and consent language and settings that are simple and transparent

- Create transparent and clear communication with users about the personal data that we collect and process, including information in culturally, age, and channel-appropriate ways about:
    - What information is being collected?
    - Who is collecting it?
    - How is it collected?
    - Why is it being collected?
    - How will it be used?
    - With whom will it be shared?
    - What will be the effect of this on the individuals concerned?
    - How long will personal data be retained?
    - Is the intended use likely to cause individuals to object or complain?
    - What are user rights related to their data?
    - Can they expect any feedback or response related to data they have provided? When?
- Ensure that consent for collecting and using personal data is 'opt in', not assumed or 'opt out'.
- Make it clear when we are relying on any other lawful basis for the collection and processing of personal data.
- Design consent processes in ways that help users understand privacy and data uses.
- Choose the most private rather than the most open settings during design.
- Disable location settings or ensure that users understand and consent if we are tracking them.
- Allow users to delete or remove their photos, comments, profiles and any other data.

Determine what systems we will use to protect, store and maintain the data

- Are we able to ensure the rights of data subjects in our system?
- Will our backend systems enable us to securely record, manage and trace consent?
- Do we have data agreements in place with any third parties who will have access to the data?
- Do we have a plan in place, with responsibilities assigned, to manage a data breach?

Tailor your tools to support the rights children have under the GDPR

Include the following in your product:

- A 'download all my data' tool to support the right of access, and right to data portability.
- A 'delete all my data' or 'select data for deletion' tool to support the right to erasure
- A 'stop using my data' tool to support the rights to restrict or object to processing; and

[5] This Annex is taken from: Girl Effect, 2018. *Digital Safeguarding Tips And Guidance*. [ebook] Available at: <https://prd-girleffect-corp.s3.amazonaws.com/documents/Digital_Safeguarding_-_FINAL.pdf?AWSAccessKeyId=AKIAIWVYO5R6RMTXA2NA&Signature=9uRyrXXcikvwAYR9M1DivZniJ2w%3D&Expires=1586867812> [Accessed 14 April 2020]. Pg. 22.

- A ‘correction’ tool to support the right to rectification.

Used together with privacy settings, such tools should help to give children control over their personal data.

Annex 2: Tips for keeping phones safe for girls

Safeguarding tips for all phones

- Password protect phones and devices with a PIN that differs from the factory setting and which is unknown to others.
- Do not give your number out to anyone you don't completely trust.
- Disable Bluetooth and GPS when not using them.
- Do not store sensitive information on your phone.
- Do not send messages with sensitive information in them.
- Never leave your phone unattended.
- Never sign into your accounts on someone else's phone.
- Look out for unknown programmes and running processes, strange messages and unstable operation.
- If you don't know or use some of the features and applications on your phone, disable or uninstall them if you can.
- Don't pick-up and answer calls from numbers you don't recognise.

Smart phone-specific tips

- Disable Wi-Fi, mobile data, Bluetooth and GPS when you are not using them.
- Educate yourself about the apps on your phone, know exactly what they do and what information they store.
- Turn off location services throughout the apps on a phone, but in particular, on the camera and on the social media.
- DO NOT log into Google Maps. Google Maps tracks your every movement unless you turn it off, and you can be tracked remotely through the app.
- Delete apps which store location or any other information.
- When using someone else's device or a public computer, sign in with precaution. If you do - delete your history and saved passwords.