

English Connects Programme

Digital Safety and Online Risks

MARCH 2023

Setting the context

- The rapid acceleration of digital technology over the last few years, particularly through the pandemic, has changed the safeguarding landscape
- Online abuse has increased dramatically:
- The prevalence of ICT-facilitated violence against women and girls globally may range between 16% to 58%.
- Although there is limited research that brings attention to how this issue manifests within Africa, the existing literature shows that cyberbullying has been widely reported across several Sub-Saharan African countries including Botswana, Ethiopia, Ghana, South Africa, Senegal, Nigeria, and Uganda, to name a few.
- Another study showed that more than 45% of 18- to 45-year-old female participants that used Facebook or Twitter in West and Central Africa reported having experienced some form of gender-based violence (GBV) on social media.
- This is a significant issue within Africa where more than 139 million people used Facebook as of 2018.
- Low recognition of technology-facilitated abuse (or even wider forms of abuse) as criminal acts.

What is Online abuse / exploitation?

Online abuse is any type of abuse that happens on the internet, facilitated through technology like computers, tablets, mobile phones and other internet-enabled devices

- It can happen anywhere online that allows digital communication, such as:
 - Social networks/platforms – Facebook/Instagram/Twitter
 - Text messages and messaging apps – Whatsapp/Kick/Snapchat
 - Email and private messaging – MSN/Gmail/Instant messenger/
 - Online chat sites/apps – Skype/Zoom
 - Comments on live streaming sites – Youtube/Instagram
 - Voice chat in games – PlayStation/Xbox

Online abuse

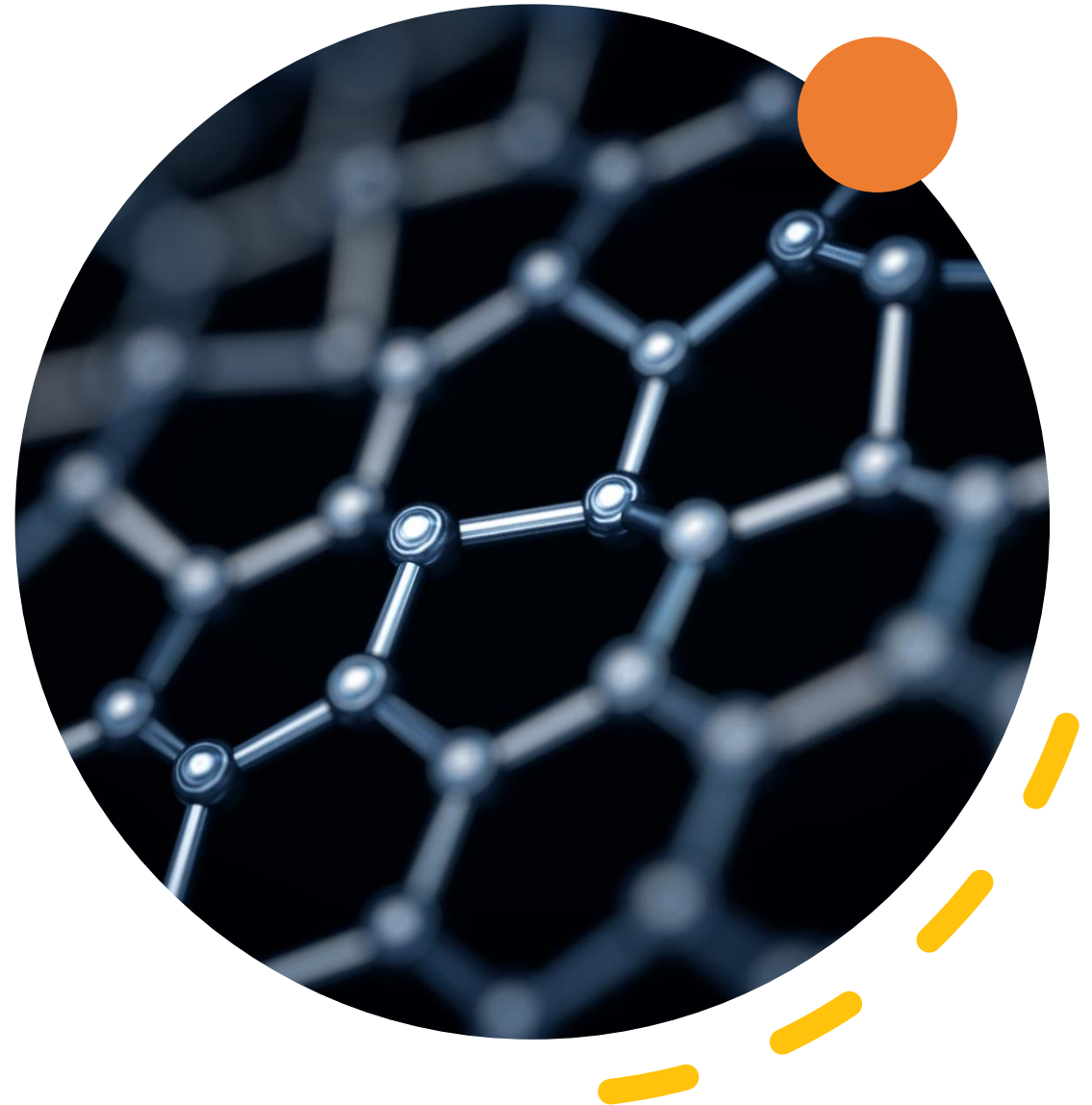
Children and adults can be re-victimised (experience further abuse) when abusive content is recorded, uploaded or shared by others online. This could happen if the original abuse happened online or offline.



Images can never be removed from every site and therefore they remain and these images are viewed over and over again with a forever digital footprint



Behind every image/video is a victim who has been abused



Online Safeguarding Risks:

Cyberbullying

Sexual and financial exploitation

Sexual abuse – contact and non contact

Grooming – children and adults

Webcam – facilitating abuse

Sextortion – extortion to create and share indecent images/videos/chat

Blackmail – sexual/financial/emotional

Digital Risks

- Children are particularly at risk in online environments due to their developmental vulnerabilities.
- However, the risks can also be relevant for adults too who may also face adversities online
- Take a few minutes to consider & note general online risks that children / Young people or Adult students may encounter in everyday settings.

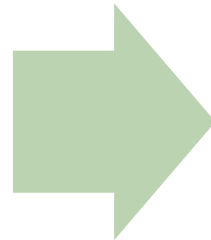


shutterstock.com · 1305029218

Contact risk – This is the risk of becoming a victim of interactive situations. This includes being bullied, harassed or stalked online, as well as the risk of grooming for sexual exploitation. The online environment creates opportunities for offenders to exploit those who may be vulnerable due to their age or circumstances. This exploitation may be initiated online but can result in online and/or offline acts of abuse.

Content risk – This includes hateful content, harmful content, illegal content and disinformation. Many online platforms can expose users to violent, extremist, hate, self-harming, or other forms of undesirable content online.

Conduct risk – This is where simply being online encourages users' own risky behaviour or conduct. This can include participating in harmful interactive situations such as encouraging or participating in online bullying, or it can include oversharing personal information which has a longer-term impact on reputation. It can include disclosing experiences, or aspects of identity or sending sexual images that are shared onwards.



Consumer risks – This includes a range of risks including marketing and commercial profiling, financial and security risks. These include non-transparent advertising, and commercial pressure on users as well as privacy issues where users may share data to participate online leading to commercial or other content profiling based on their data. This risk also includes the way that digital services can be designed to be addictive.

Our Collective Responsibilities

- Supporting our customers, staff, and beneficiaries in digital spaces to work safely and effectively online.
- Promoting best practice in digital safety with guidance and tools.
- Ensuring that all users know what should be reported and how.
- Following the guidance in digital interactions with learners and beneficiaries.



shutterstock.com • 143745571

Supporting and encouraging users to manage their privacy:

The British Council should seek to support users to make informed choices about their privacy.

For children and adults this will include encouraging users to think about the data they are sharing and to be aware of the options and advantages of using privacy settings and blocking unwanted contacts.

Top Tip – Always clear cookies on public computers and regularly clear your cookies on your internet browser

Find a guide on 'how to clear cookies' on your internet browser in the notes below.

Making sure everyone knows how and where to report concerns:

- 1. Inform the safeguarding team of what you have seen, and they will advise you. Do not share the material as part of the referral.**
- 2. Safeguarding concerns about a child or adult - This includes things that occur during lessons or in any digital interactions that you become aware of.**
- 3. Teachers, staff, and people we work with, must report safeguarding concerns or incidents to their safeguarding focal point / British Council primary contact who will refer onwards to the British Council safeguarding team - safeguarding@britishcouncil.org**

Resources

- [Digital Safeguarding Core Guidance](#)

Outlines the key risks faced by adults and children in digital interactions and sets out core guidance to enable British Council staff and partners to uphold safeguarding when engaging online.

- [Digital Safeguarding Statement.](#)

This statement outlines how we will work to create a safe digital and online engagements.

- [Digital Safeguarding Community Standards](#)

The community standards describe and articulate our expectations of behaviour and conduct of our clients, beneficiaries and partners etc when engaging digitally.

- [Digital Safeguarding Risk Assessment](#)

This tool is designed to help users to ensure that they are managing digital risks and following best practice in online interactions. It can also be used to help ensure that staff and partners are applying relevant and useful mitigations to manage risks.

- [Digital Safeguarding App Guide](#)

This guide provides relevant information to help users identify risks in using certain popular apps and how to mitigate some of the risks.

- [Digital Safeguarding Resource Library](#)

A collection of relevant Digital Resources that can be utilised in different ways across the business

- [Online Safety Advice 8 - 12 Year Old](#)

Safety information for 8 – 12 years can be used for poster\leaflet\ workbook content

- [Online Safety Advice 13+ Year Old](#)

Safety information for 13+ can be used for poster\leaflet\ workbook content

- [Digital Safeguarding Advice for Adults](#)

Safety information for Adults can be used for poster\leaflet content etc

- <https://hwb.gov.wales/keeping-safe-online/in-the-know/telegram-messenger/>

Video resources

- [Digital Safeguarding Film - 4 Min Version](#)
4 Minute overview of the need for digital safeguarding and the importance to the British Council
- [Digital Safeguarding Film - 4 Min Version \(Subtitles\)](#)
4 Minute overview with subtitles.
- [Digital Safeguarding Film - 8 Min Version](#)
8 Minute overview of the need for digital safeguarding and the importance to the British Council.
- [Digital Safeguarding Film - 8 Mins Version \(Subtitles\)](#)
8 Minute overview with subtitles.
- [Animation for Children - how to stay safe online](#)
Animation for children giving tips on how to stay safe online.
- [Animation for Children - how to stay safe online \(Subtitles\)](#)
Animation for children giving tips on how to stay safe online with subtitles.

The image features a central graphic of a paint splatter. The splatter is composed of numerous small, irregular droplets and larger blotches of color, including purple, blue, cyan, green, yellow, orange, and red. The colors transition from purple on the left to red on the right, with intermediate shades of blue, green, and yellow. The splatter is set against a plain white background. Overlaid on this colorful background is the text "Thank You!" in a large, white, bold, sans-serif font. The letters have a slight 3D effect, appearing to float slightly above the splatter. The exclamation point is also white and matches the font style.

Thank You!