Youth Action Alliance (YAA)

Protecting Children from Online Abuse Guidance and E-Safety Policy

A: Youth Action Alliance, The Hut, 202 Wornington Road, London, W10 5RE
T: 020 8964 3149 **E:** info@youthactionalliance.org **W:** www.youthactionalliance.org

Contents

A: Youth Action Alliance, The Hut, 202 Wornington Road, London, W10 5RE
T: 020 8964 3149 **E:** info@youthactionalliance.org **W:** www.youthactionalliance.org

1. This Guidance

This guidance has been produced by YAA based on NSPCC good practice guidance to inform employees and volunteers who work for the organisation about the types, impact, risk of and ways of dealing with online abuse. It is an accompanying document to YAA's Safeguarding & Child Protection Policy. Employees and volunteers should consult the Safeguarding & Child Protection Policy for information about what to do if you think a young person or vulnerable adult is at risk from a safeguarding matter and gives information about how to report an incident and who to contact.

2. Definition

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 (Department for Education, 2018; Department of Health, 2017; Scottish Government, 2014; Welsh Assembly Government, 2018).

It can happen anywhere online that allows digital communication, such as:

- social networks
- text messages and messaging apps
- email and private messaging
- online chats
- comments on live streaming sites
- voice chat in games.

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

Children and young people may experience several types of abuse online:

- bullying/cyberbullying
- emotional abuse (this includes emotional blackmail, for example pressuring children and young people to comply with sexual requests via technology)
- sexting (pressure or coercion to create sexual images)
- sexual abuse
- sexual exploitation.

Children and young people can also be groomed online: perpetrators may use online platforms to build a trusting relationship with the child in order to abuse them. This abuse may happen online or the perpetrator may arrange to meet the child in person with the intention of abusing them.

3. Impact of Online Abuse

Whether abuse happens online or offline it can have a long-lasting impact on a child's overall wellbeing. Online abuse can lead to:

- anxiety
- self-harm
- eating disorders

- suicidal thoughts (HM Government, 2017).

Research shows that cyberbullying has similar effects to offline bullying. It can lead to:

- falling behind at school
- depression
- anxiety
- other mental health difficulties.

Cyberbullying can make children feel more frightened and helpless than bullying that happens offline. Contact from cyberbullies can happen at any time, anywhere and this can make children feel like they can't escape (Munro, 2011).

Online child sexual abuse has as much of an impact on a child or young person as sexual abuse that takes place offline only (Hamilton-Giachritsis et al, 2017). Effects of online sexual abuse can include:

- self-blame
- flashbacks or intrusive thoughts
- difficulties sleeping
- nightmares
- extreme tiredness
- difficulties concentrating
- difficulties keeping up with school work
- behavioural problems at school
- depression
- low self-esteem
- social withdrawal
- panic attacks and anxiety
- eating disorder or eating difficulties
- self-harm (Hamilton-Giachritsis et al, 2017).

However, experiencing abuse online and/or using technology can cause additional effects:

- young people may be afraid of sexual images being shared online or being viewed in the future, particularly if the perpetrator has made threats about sharing sexual images in order to blackmail the young person into complying with further abuse
- being filmed can lead some young people to feel uncomfortable around cameras
- young people who have been in constant contact with the person who abused them via digital technology can become very fatigued – especially if they were in contact during the night. They may also feel powerless and frightened.
- some young people who were abused online feel that this made them more vulnerable to further abuse by sexualising them, leading them to drink heavily or take risks or reducing their sense of self-worth and confidence (Hamilton-Giachritsis et al, 2017).

Speaking out

A child or young person may be reluctant to speak out about the abuse they've experienced

online.

They may:

- not understand that they are being abused
- feel dirty and ashamed
- be too embarrassed to share the sexual details of what's happening to them
- be afraid because of threats of violence from the abuser
- have been told by the abuser that they won't be taken seriously
- have established an emotional attachment with the abuser and don't want to get them into trouble (NSPCC and O2, 2016).

They may also blame themselves for the abuse and not expect to get any support. This might especially be the case if they have experienced unsupportive approaches from school, peers and family (Hamilton-Giachritsis et al, 2017).

Their abuser may also have threatened to share sexual images of them if they tell anyone about the abuse. This means they might be frightened to speak out.

4. Recognising Online Abuse

It can be easier for perpetrators to initiate, maintain and escalate abuse through digital technology because it gives them:

- easier access to children and young people through social media and digital messaging
- anonymity – it's relatively easy to create anonymous profiles on online platforms or pretend to be another child
- children may have a false sense of safety online which means they're more likely to talk to strangers than in the offline world (Hamilton-Giachritsis et al, 2017).

Children can be at risk of online abuse from people they know as well as from strangers. Online abuse may be part of abuse that's taking place in the real world such as bullying or an abusive relationship. Or the abuse may happen online only.

A child who is experiencing abuse online may:

- spend much more or much less time than usual online, texting, gaming or using social media
- be withdrawn, upset or outraged after using the internet or texting
- be secretive about who they're talking to and what they're doing online or on their mobile phone
- have lots of new phone numbers, texts or e-mail addresses on their mobile phone, laptop or tablet.

Risks

EU Kids online has developed a framework of risks called the 3Cs. This outlines the risks a child may experience when they are online.

Content

Age-inappropriate content that a child may come across online could be:

- commercial – such as adverts, spam or sponsorship
- aggressive – such as violent and hateful content
- sexual – inappropriate or unwelcome sexual content
- content that promotes negative values – for example biased, racist or misleading information.

Contact

If a child is actively engaged in the online world, they may become involved in interactions that could be harmful to them. This could be:

- commercial – such as tracking the sites a child has looked at or harvesting their personal information
- aggressive – for example being bullied, harassed or stalked
- sexual – receiving sexualised requests from others or being groomed
- contacts who promote negative values – for example making 'friends' who persuade a child to carry out harmful activities.

Conduct

Without meaning to, a child may behave in a way that puts them and/or others at risk. For example they may become involved in:

- inappropriate commercial activity - illegal downloading, hacking, using the dark web or getting involved in financial scams
- aggressive behaviour – bullying or harassing someone else
- sexualised behaviour – creating or uploading indecent images
- creating content that promotes negative values – providing misleading information to others (Hasebrink et al, 2009).

Vulnerability factors

There's no clear set of factors that make children and young people more likely to be affected by online abuse. Different circumstances in a child or young person's life may combine to make them more at risk. But some factors can make children and young people more vulnerable to abuse.

Age

Pre- and early teens are an especially vulnerable age for children online. From 11-12, children start to explore and take risks online, but they haven't yet developed the skills needed to recognise danger or build resilience against things that might upset them (Munro, 2011; Livingstone and Palmer, 2012).

Children aged 9-16 are particularly vulnerable to:

- seeing sexual images online
- seeing online content that promotes potentially harmful behaviour, such as pro-anorexia or self-harm sites
- being bullied online (Mascheroni and Cuman, 2014).

At this age, young people may be starting to explore their sexuality too. They might find adult pornography online or start online relationships with people they don't know (Munro, 2011; Livingstone and Palmer, 2012).

Teenagers may be more vulnerable to cyberbullying than younger children (NSPCC, 2015).

Gender

Boys and girls may differ in the types of risks they take online and the risks they are exposed to.

EU Kids Online research (Livingstone et al, 2009) found that boys are more likely to:

- look for offensive or violent pornography online, or be sent links to pornographic websites
- meet someone offline who they have talked to online
- give out personal information.

The research also found that girls are more likely to:

- be upset by violent or offensive online pornographic content
- chat online with people they don't know
- receive unwanted sexual comments
- be asked for personal information (Livingstone et al, 2009).

Research also suggests that girls are more likely to experience ongoing cyberbullying than boys (Cross et al, 2009).

Vulnerability to online grooming

Loneliness, social isolation and family problems may make young people more vulnerable to being groomed online (NSPCC and O2, 2016). Groomers may initially be attentive and sympathetic, which means a young person who is experiencing difficulties may quickly see them as a trusted source of support, especially if they are pretending to be another child.

Special educational needs or disability

Children with special educational needs (SEN) or disabilities are particularly vulnerable to online abuse (Livingstone and Palmer, 2012). A child with SEN or a disability may:

- have low self-confidence, seeing themself as an 'outsider'
- lack strong peer networks and be less likely to tell a friend when they experience upsetting things online
- have more unsupervised time online, with fewer structures and boundaries (Livingstone and Palmer, 2012).

5. Responding to Online Abuse

Youth Action Alliance has a Safeguarding and Child Protection Policy that sets out what action staff and volunteers should take if they have concerns about a child's safety online.

Reporting

If you think a child is in immediate danger, contact the police on **999**. If you're worried about a child but they are not in immediate danger, you should share your concerns.

- **Follow YAA's Safeguarding & Child Protection Policy**.
- **Contact the NSPCC Helpline** on 0808 800 5000 or by emailing help@nspcc.org.uk. Our trained professionals will talk through your concerns with you and give you expert advice.
- **Contact your local child protection services**. Their contact details can be found on the website for the local authority the child lives in and in YAA's Safeguarding Young People and Vulnerable Adults Policy.
- **Contact the police.**
- If your concern is about online sexual abuse, you can make a report to the Child Exploitation and Online Protection (CEOP) command.
- The police and NSPCC will assess the situation and take action to protect the child as appropriate. This may include making a referral to the local authority.
- Services will risk assess the situation and take action to protect the child as appropriate either through statutory involvement or other support. This may include making a referral to the local authority.

Reporting online child abuse images

It's against the law to produce or share images of child abuse, even if the image was self-created. This includes sharing images and videos over social media.

If you see a video or image that shows a child being abused:

- Don't comment, like or share the video or image, as this will distribute it further.
- Report it to the website you've seen it on.
- Report it to the police.
- Contact the NSPCC helpline on **0808 800 5000 and we'll report it to the police for you.**
- If the image or video involves the sexual abuse of a child, report it to the Internet Watch Foundation (IWF) who will take steps to get it removed from the internet.
- If a child has taken a sexual picture of themselves and lost control of it, they can contact Childline who will work with the IWF to get it taken down.
- Some images and videos may appear old but it's still important to report them. You can help prevent the video being shared further by alerting the person sharing the video that it's been reported to the authorities.

Responding to cases of online abuse

When responding to cases of online abuse, it's important for adults to understand the impact it can have on a young person's wellbeing. They should:

- listen calmly to what the child has to say
- remember that the young person may be embarrassed and/or ashamed
- be non-judgmental and make sure the child knows that abuse is never their fault.
- It's also important for adults to understand that online and offline abuse are often

entwined and ask tactful questions when the child is ready to understand the context of the abuse. This will enable them to provide the child with the right support.

- Parents should be informed about cases of online abuse unless to do so would put a child at further risk of harm. They may need additional support to understand what has happened and how best to help their child.
- In cases where the child or young person has gone to the police about online abuse, it's important for them to:
- fully explain the legal process in a way the child or young person can understand
- be friendly, reduce formalities as much as possible and make the child feel comfortable
- offer the child choice where possible, for example:
    - how they want to give evidence
    - the gender of the key police officer(s) involved
    - what other professionals they would like to be involved
- provide a consistent officer to work with the child throughout the case
- keep in contact with the child and their family regularly and provide regular updates on the progress of the case (Hamilton-Giachritsis et al, 2017).
- Children who have experienced online abuse need to be provided with ongoing support.

6. Preventing Online Abuse

To prevent child abuse online, it's essential for those who work with children and young people to help them:

- learn about the risks associated with online activities
- develop the awareness and skills needed to keep safe online
- learn about healthy relationships, abuse and consent from a young age
- know where to go for help – and recognise that they can help themselves too
- know how to report unacceptable activity or behaviour (UNICEF, 2011; Hamilton-Giachritsis et al, 2017).

Youth Action Alliance has written policies and procedures that promote online safety.

It's also important to support parents to know how to keep their children safe online.

Keeping children and young people safe online

While the internet is often a positive part of children's lives, young people can be vulnerable to abuse and inappropriate content in the online world. There are actions parents, carers and organisations can take to keep online spaces safe for children.

- Make sure you're available to talk to children and young people about anything worrying they experience online.
- Recognise how important the online world is to children and young people. Talk to them about it.
- Make sure online safety is an ongoing part of your work with children and young people, not just a one-off session.
- Set rules for the use of online platforms in your organisation. Make sure children and young people understand them and are involved in setting them.

- Use technical solutions to manage access to online platforms in your organisation. Make sure children and young people know about this and understand why you've put them in place.
- Talk to children and young people about their own privacy settings and help them manage what other people can find out about them online.

Building children's online safety skills

It's important that children are given the knowledge and skills needed to keep themselves safe online, to build their own resilience (UNICEF, 2011; Livingstone and Palmer, 2012).

The NSPCC has created guides for parents and carers on:

- How to talk to your child about online safety
- Online games: helping children to play safe
- Keeping children safe from sexting and online porn.

The UK Council for Internet Safety (UKCIS), in partnership with the NSPCC, has developed a framework for anyone who works with children and young people to support them to be safe in the digital world (UKCIS, 2018).

Areas covered in the guide include:

- self-image and identity
- online relationships
- online reputation
- online bullying
- managing online information
- health, wellbeing and lifestyle
- privacy and security
- copyright and ownership (UKCIS, 2018).

Preventing online grooming

The Stop TIME Online activity pack (NSPCC Cymru/Wales and Swansea University, 2017) gives professionals and young people a better understanding of the strategies online groomers use to build trusting relationships with young people. The materials can be used during one-to-one or small group work sessions with children and young people aged 8 to 18 who are at risk of online grooming.

Online behaviour

Everyone who works or volunteers for Youth Action Alliance should follow an online code of conduct. This includes:

- not engaging with children on social networking sites or through mobile devices
- keeping personal information private online
- considering the long term implications of content posted online
- not uploading or posting inappropriate offensive or illegal content on any online space.

We also promote healthy online behaviour amongst the children and young people who we

work with. Youth Action Alliance also uses online safety agreements where required.

7. Key Legislation for Online Abuse

Across the UK, criminal and civil legislation aims to prevent a range of abusive activities online including:

- stalking
- harassment
- improper use of a public communications network
- sending indecent, offensive, false or threatening communications
- sending private sexual photos or videos of another person without their consent.

Online harassment

Throughout the UK, the Communications Act 2003 makes it an offence to make improper use of a public communications network. Section 127 specifically makes it an offence to send an electronic message that is grossly offensive or of an indecent, obscene or menacing character.

In England and Wales, the Malicious Communications Act 1988 makes it an offence to send a communication with the intention of causing distress or anxiety.

Online sexual abuse

Across the UK, the legislation setting out sexual offences also applies to online child sexual abuse, including:

- sexual communication with a child
- causing or inciting a child to engage in sexual activity
- causing a child to watch a sexual act
- paying for sexual services of a child
- causing or inciting sexual exploitation of a child
- engaging in sexual activity in the presence of a child.

Trafficking and modern slavery legislation across the UK makes it an offence to traffic and/or enslave children for sexual exploitation and makes provisions for sentencing offenders. These can also apply to trafficking children for online sexual exploitation.

Sexting

Young people may exchange sexual messages and self-generated sexual images or videos through a mobile phone network or the internet (sexting).

Online grooming

It can be difficult for the police and legal professionals to make legislation apply to online grooming.

For example it can be difficult to prove that grooming messages are intended to cause distress or anxiety because perpetrators usually send messages that aim to build trust and rapport with a child.

Throughout the UK, criminal and sexual offence legislation makes grooming and meeting a child following sexual grooming offences.

Legal responsibilities for website hosts and social media platforms

In England and Wales, the Defamation Act 2013 makes the website host responsible for removing defamatory material posted to a site.

Section 103 of the Digital Economy Act 2017 requires social media platforms across the UK to follow a code of practice which sets out the actions they must take to protect individuals from bullying, intimidation and insulating behaviour online.

In April 2019 the Department for Digital, Culture, Media and Sport (DCMS) and the Home Office opened a public consultation on their Online Harms White Paper. This sets out the measures the government intends to take to keep UK users safe online, including a new regulatory framework for online platforms (DCMS, 2019).

The Information Commissioner's Office's (ICO) Age appropriate design: code of practice for online services sets out 15 standards that providers of online products or services likely to be accessed by children should comply with. The code explains how providers can design services that appropriately safeguard children's personal data and comply with data protection and privacy laws. The code is expected to come into force by autumn 2021, following Parliamentary approval (Information Commissioner's Office, 2020).

Key guidance

Across the UK, statutory guidance highlights the responsibility of those in the education, community and care sectors to safeguard children from all forms of abuse and neglect including online abuse:

- Child protection legislation and guidance in England

There is also more specific guidance for people who work with children about safeguarding children from online abuse.

Keeping children safe from online abuse

The UK Home Office has published guidance aimed at tech firms, the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse. The guidance is comprised of 11 actions that online companies should take to tackle online sexual exploitation, including on tackling child sexual abuse material, online grooming and livestreaming of child sexual abuse. The guidance was developed in collaboration with the Governments of Australia, Canada, New Zealand and the USA (Home Office, 2020).

The UK Council for Internet Safety (UKCIS) has produced a framework (PDF) for people who work with children across the UK that highlights the digital skills and knowledge children need to stay safe online. It includes discussion around:

- online relationships
- online reputation
- online bullying (UKCIS, 2018).

The Home Office has developed an Online abuse and bullying prevention guide (PDF) for

those who work with young people in England and Wales. This aims to help them understand the types of online abuse, its consequences and where to go for help. Topics covered include:

- threatening behaviour
- cyberbullying
- online grooming (Home Office, 2015).

Our online safety e-learning course helps people who work with children across the UK understand what they need to do to safeguard children online.

Key policy

The government's Online Harms white paper sets out the measures the government intends to take to keep UK users safe online, including:

- establishing a new statutory duty of care and regulatory framework to ensure online platforms take responsibility for the safety of their users
- a new independent regulator to implement, oversee and enforce the regulatory framework and raise awareness about online safety (DCMS, 2019).

8. Youth Action Alliance E-Safety Policy

E-Safety Policy Statement

Youth Action Alliance's e-safety policy and procedures apply to all staff, volunteers, Board of Trustees and anyone working on behalf of YAA.

The aim of the policy is to:

- Protect children and young people who receive YAA's services and who make use of information technology (such as mobile phones and the internet) as part of their involvement with us
- Provide staff and volunteers with the principles that guide our approach to e-safety
- Protect professionals
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use information technology

We recognise that:

- The welfare of the children, young people and vulnerable adults who come into contact with our services is paramount and governs our approach to the use and management of information communications technologies

We will promote e-safety by:

- Having procedures that provide clear and specific directions to staff and volunteers on the appropriate use of ICT
- Supporting and encouraging the children and young people using our service to use the opportunities offered by mobile phone technology and the internet in a way that keeps themselves safe and shows respect for others
- Educating and providing information for parents/carers
- Supporting and encouraging parents and carers to keep their children safe online and when using their mobile phones
- Incorporating statements about safe and appropriate ICT use into the codes of conduct for staff and volunteers and for children and young people
- Having an e-safety agreement with children and young people
- Using our procedures to deal with any inappropriate ICT use, complaints and/or allegations by anyone working for YAA or using our services
- Informing parents and carers of incidents of concern as appropriate
- Regularly reviewing and updating the security of our information systems
- Ensuring that images of service users are only used after their consent has been obtained, and only for the purpose for which consent has been given, and in line with the YAA Data Protection Policy

We will handle complaints regarding e-safety by:

- Taking all reasonable precautions to ensure e-safety
- Giving staff/volunteers and children/young people information about infringements in use and possible sanctions
- Recording any E-Safety incidents using the E-Safety Incident Monitoring Form

Sanctions include:

- Interview with a member of staff
- Inform parents/carers
- Removal of internet or computer access for an agreed period of time
- Referral to local authority/police

The lead worker will be the first point of contact for any e-safety related complaint and a YAA E-Safety Incident Monitoring Form will be completed.

Any complaint about staff/volunteer's misuse will be referred to the manager and may result in formal disciplinary proceedings. Complaints of cyber-bullying are dealt with in accordance with our anti-bullying policy.

Concerns related to child protection are dealt with in accordance with our Safeguarding & Child Protection Policy and procedures.

Last Reviewed: April 2024
Next Review: April 2025