Online Safety

Introduction

Welcome to your course on ‘Online Safety’ written in partnership with Childnet International. Childnet is a non-profit organisation working with others to help make the internet a great and safe place for children.

The purpose of this course is to help you understand:

- why children and young people spend time online
- the 4Cs of potential online harm
- how to prevent online harm
- how to respond to reports of online safeguarding concerns.

Role of staff

As a member of school staff, you have a crucial role when it comes to ensuring the online safety of children and young people. Schools have a dual responsibility to:

- make sure they have policies and procedures in place that range from filtering and monitoring access to embedding online safety into the curriculum
- support young people in navigating through the complexities of the online world.

Online safety forms a part of your safeguarding duties to all children and young people you work with. If you are worried about a child or young person, then you should follow the school’s child protection policy and procedures.

It is vital that all those working with children and young people:

- have an awareness of risks and trends online
- have appropriate online safety training
- work with and learn from children and young people about what they are doing online
- encourage children to ask questions and listen to their experiences and views
- are aware of their own online reputation
- make sure that any technology used within the school is used appropriately
- ensure children have appropriate routes to support and reporting.

Module 1 – Understanding the online world and potential online harms

Why do people spend time online? (What can it offer?)

From your experience with working with children, you may find they go online for a variety of reasons.

> **Reflective question**
> What do you use the internet for in your professional time, and your personal time?

When you compare the lists between you and children, you may see that that they are very similar.

You may use the internet to:

- communicate with friends and family, for example, through social media
- make purchases
- learn new skills

- participate in gaming
- utilise online services, for example, banking
- communicate with others that have similar interests.

You may find you do these things in both a professional and personal capacity.

Similarly, young people use the internet and technology partly because it is a tool that they can benefit from but also as something which they are passionate about and enjoy. Young people enjoy watching videos, playing games, chatting with friends and family, creating and sharing content, learning new skills, listening to music and building communities.

Scenarios

George

School - *George is 15 years old and has been asked to write a letter of application for his work placement. He uses AI to help him.*
Personal - *George enjoys playing football video games on his games console. He uses voice chat whilst he plays to communicate with online friends across the country. George spends time on social media talking to his school friends.*

Aadhila

School - *Aadhila, 17, researches her assignments using online sources, participates in virtual classroom discussions, and submits homework through her school's online platform.*
Personal - *Aadhila chats with friends online and shares her creative projects with online art communities.*

A young person's online activity can influence their life 24 hours a day, 7 days a week. Many children and young people report feeling 'disconnected' from the world if they cannot go online, but they can often be unaware that what they do online can affect them offline. It is important to recognise that young people do not tend to differentiate between life online or offline; it is all part of their life.

Builds social connections

- ***George** has expanded his friendship group and has reduced his feelings of loneliness.*
- *By expanding her social connections and sharing her creative projects **Aadhila** has learnt new skills.*

Education

- ***George** has learned new skills whilst gaming and has found his concentration has improved.*
- *By participating in virtual classroom discussions **Aadhila** has been able to have a deeper understanding*
  of the topics she is researching.

By understanding the different risks that occur across all platforms, you will be better informed to support students in whatever they enjoy doing online.

Reflective question
From your previous experience and existing knowledge, what online harms are you aware of?

Potential online harms could include, but are not limited to:

- violence
- grooming
- online bullying
- sexual or adult content
- non-consensual image sharing
- hearing inappropriate language
- encouragements to self-harm or suicide ideation
- extremist political, social, or religious views.

4Cs model

It is unrealistic to expect all those working with children and young people to know and keep up to date with all the apps and games children access. However, understanding the basic concepts of social media and gaming and how young people access them will help you to understand the potential risks. This approach will also support professionals in understanding risks as they evolve alongside emerging technology, for example the use of generative AI (e.g. Chat GPT and Snap AI). It is also important to know how risks can run across multiple platforms and experiences and how to minimise them.

Online safety risks can be categorised into four areas – Content, Contact, Conduct and Commerce.

This is a useful frame to help understand each risk and the potential different dimensions online safety concerns can take. However, it must be noted that there is increasing overlap between categories and risks are often multi-faceted, sitting across two or more of the areas.

It should also be noted that the breadth of issues classified within online safety is considerable and ever evolving.

Content

Reflective questions
What are children and young people able to access and experience online?
What **content** would be of a safeguarding concern online?

The **Content** risk refers to what a child might see online, for example, being exposed to illegal, inappropriate, or harmful content.

This can include but is not limited to:

- pornography
- fake news and misinformation
- content which encourages self-harm and suicide
- online hate, for example racism, misogyny, ableism, islamophobia, antisemitism, homophobia, biphobia and transphobia.
- radicalisation and extremism.

Content risks can include:

Pornography

Definition
Online pornography can be images or videos online of naked adults, or adults having sex or showing sexual behaviour.

Potential risk
If young people watch online pornography before they are old enough to fully understand it, or before they have learned about healthy sex and relationships in RSE lessons, they may misinterpret pornography as an accurate representation of healthy sexual behaviour. Pornography may not show consensual or safe sexual relationships, often portrays violence especially against women and girls, and features adults who young people may compare their own body and appearance to.

Scenario
Kumal first saw pornography when he was 11 years old and by accident after a friend sent him a link. He found the videos confusing and distressing but was also curious because other people seemed to like them. Now he's 16 and sexually active with his girlfriend. He thinks about trying out things he first saw in porn but isn't sure his girlfriend really enjoys it.

Misinformation/disinformation

Definition
Misinformation refers to false or misleading information that is shared without the intent to deceive. **Disinformation** is content that is deliberately created to spread false or misleading information with the intention to deceive and manipulate.

Potential risks
- Fake news: False reports about celebrity deaths or political events, influencing opinions and causing panic.
- Doctored images: Altered photos portraying individuals in compromising situations to tarnish their reputation.
- Conspiracy theories: Baseless claims, like the "flat Earth" theory or unfounded health-related conspiracies, misleading people.
- Clickbait headlines: Sensationalised titles designed to attract clicks, often distorting the actual content of the article.
- Out-of-context quotes: Sharing partial statements to misrepresent someone's views or intentions.
- Deepfake videos: Realistic yet fabricated videos created using AI which shows people saying or doing things they never did.
- Misleading statistics: Presenting data selectively to create a false impression about a situation.
- Phishing scams: Deceptive emails or websites tricking users into revealing personal information.
- Rumours: Spreading unverified information as facts through social media platforms.

Scenario
14-year-old Alex reads a sensational online story about a new law banning video games for children under 14 years. Believing it to be true, Alex spreads the news at school, causing an uproar. Eventually, a teacher intervenes, showing the importance of verifying information before accepting and sharing it.

Teaching students to critically assess sources, recognise manipulation tactics, and foster a healthy scepticism is essential in combating the spread of misinformation and disinformation in the online world.

Contact

The **Contact** risk is being subjected to harmful online interactions with other users; for example: peer to peer pressure, online users contacting children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Technology is an integral part of children and young people's way of building and maintaining friendships. This can have positives, such as maintaining contact with friends who have moved away, and they do not see in-person as often. However, it can also present challenges and make managing friendships more difficult. For example, for some young people, how many likes and followers they have can influence how they are feeling.

Online contacts may or may not be who they say they are. Some may have ill intent; for example, sexual predators who attempt to groom children with the aim of meeting them offline. They may also be people who threaten, intimidate or bully others.

Education about online contact needs to address the risks of meeting up with someone you only know online as well as communicating with them online. Some strangers may exploit children through the internet to obtain indecent images or videos so they can continue to exploit a child.

Online platforms can be a tool for individuals or groups to:

- bully and intimidate children and young people
- groom children and young people
- engage in sexting or coerce children into sending sexual images.

Scenarios

George receives a private message on social media from someone who claims to be from his school who is arranging study sessions. Their name isn't familiar, but it is a large school.

Aadhila has joined a social media group and has started to message some of the group privately. She feels some of their comments are derogatory and aimed at her because she is a female.

George uses his social media to start to chat to a girl he knows and would not have normally had the confidence
to do this.

Key points

- *George has linked up with someone he does not know so could be at risk of exploitation.*
- *Aadhila feels intimidated by the group she has joined.*
- *George has started to build up a friendship with someone he would not normally have had the confidence to speak to face to face.*

Contact risks can include:

Online bullying/Cyberbullying

Definition

Online bullying, or cyberbullying, is when someone uses the internet to target and deliberately upset someone. Cyberbullying often happens on personal devices that young people have continuous access to.

This means it can happen anywhere and at any time, so it can feel like it's hard to escape. Some bullying takes place anonymously, so the young person doesn't know who is targeting them. The bully could be either someone that they know or a stranger.

Potential risk/impact

Any child can be bullied online. Some children can be seen as an easier target and so can be more at risk.

Some children may also be targeted because of their:

- sexual orientation
- race or ethnic background
- disability
- gender.

A child experiencing bullying will often feel scared and worried, they may become withdrawn, anxious and have low self-esteem.

Scenario

11-year-old Mia logs into her favourite social media platform, eager to connect with friends. Unbeknownst to her, a peer starts sending hurtful messages, mocking her appearance, and spreading rumours. Mia feels isolated and distressed and being online turns into a source of anxiety.

Grooming

Definition

Online grooming is where someone makes contact with a child online and builds up their trust with the intention of exploiting them and causing them harm.

Potential risk

Harm caused by grooming can be sexual abuse, both in person and online, and exploitation to obtain sexually explicit images and videos of the child. Grooming techniques could also be used to radicalise someone or to obtain financial information from the child or their family.

Scenario

Filip, a 15-year-old boy, joins an online gaming community. He befriends a seemingly friendly player named "Jake". Jake gains Filip's trust, showering him with attention and compliments. The relationship transforms, crossing boundaries Filip feels uncomfortable with. Filip feels afraid and confused but he is too scared to tell anyone as he fears they will think he is being silly.

> **Reflective question**
> In your experience, what other types of **contact** would be a safeguarding concern online?

Conduct

The **Conduct** risk relates to the user's own online behaviour that increases the likelihood of, or causes, harm.

Examples include:

- oversharing personal information online
- making, sending, and receiving explicit images, for example, consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, and sharing other explicit images

- exposing a user to harmful content, for example, false information about self-harm or eating disorders
- online bullying.

Children and young people should be aware that their online activity can have an impact on themselves and others. They need to be educated about how to manage their online behaviour and understand the impact their behaviour can have on others. They should understand how to report any concerns they have and be supported to have the confidence to do so; for example, by being reassured that they won't be in trouble and knowing what will happen after they have made a report.

Conduct risks can include:

Oversharing personal information

Oversharing personal information online can include but is not limited to:

- location sharing
- holiday plans and updates
- information about where a person goes to school or work
- sharing contact information
- information about personal relationships.

As someone who works with children and young people, what do you think the potential risks are from the list shown?

Example answers

- **Location sharing**
  A 12-year-old posts pictures of their new home, unwittingly sharing their exact address and neighbourhood on a public social media account.

- **Holiday plans**
  A 13-year-old shares upcoming holiday plans, including dates and destinations, providing potential information for strangers to know when a house might be empty.

- **Information about school**
  A parent posts pictures of her new school uniform school making it easier for strangers to identify and track the child.

- **Contact information**
  An 11-year-old includes their phone number or email address in their online profile or comments section, unknowingly making themselves vulnerable to unwanted contact or even potential exploitation.

- **Personal relationships**
  A 14-year-old shares intimate details about family issues or conflicts with friends on a public forum, unintentionally exposing personal matters to a wider audience.

Online sexual harassment and harmful sexual behaviour

Definition

Online sexual harassment is unwanted sexual behaviour on any digital platform. It can happen between anyone online, including between children and young people. Online sexual harassment can include a wide

range of behaviours that use digital content including images, videos, posts, and messages. They can be found on a variety of different online private or public platforms.

Potential risks

There are four main types of online sexual harassment:

- **Non-consensual sharing of intimate images and videos**
  A person's sexual images and videos being shared without their consent or taken without their consent.
- **Exploitation, coercion and threats**
  A person receiving sexual threats, being coerced to participate in sexual behaviour online, or blackmailed with sexual content.
- **Sexualised bullying**
  A person being targeted by, and systematically excluded from, a group or community with the use of sexual content that humiliates, upsets or discriminates against them.
- **Unwanted sexualisation**
  A person receiving unwelcome sexual requests, comments and content.

> **Reflective question**
> In your experience, what other types of **conduct** would be a safeguarding concern online?

Commerce

> **Reflective question**
> What type of **commerce** do you think would be a safeguarding concern online?

Commerce includes risks such as online gambling, inappropriate advertising, in-game or in-app purchases, phishing and/or financial scams, including financially motivated sextortion. Financially motivated sextortion is a form of child sexual exploitation and abuse which can also be grouped under 'Contact'.

Many children and young people are at risk of being exploited by or accidentally exposed to online marketing. They may also share personal data about themselves or their parents and carers; for example, through web cookies, their online activity, or engagement with emails and pop ups.

A further risk for young people is that they do not recognise commercial messaging, advertising; for example, or promotions by influencers.

In games, players can use in-game payments to open loot boxes which contain an item of unknown value and quantity.

Commerce risks can include:

Phishing

Definition

Phishing is the sending of bogus emails, texts or social media messages that can often look like they are from an official source. They are designed to trick the recipient into giving information such as passwords and pins which can then be used for financial or personal gain.

Potential risks

Potential risks include:

- identity theft
- Being scammed, including social media spoofing and shopping scams
- Clicking on unfamiliar links that encourage you to share details

Scenario

Mrs. Anderson is concerned when she discovers that her student, Emily, 11, has unknowingly become a target of a phishing scam. A gamer on Emily's favourite platform coaxed her into clicking a link and sharing personal details.

Financially motivated sexual extortion

Definition

Sextortion is a type of blackmail when someone threatens to share nude images or videos of, or sexual information about, someone online unless they are paid money or agree to do something else for them, such as send more images.

Sextortion is a crime and can be committed by an individual or a group of people working together.

Potential risks

Potential risks include:

- Feelings of distress, fear, and isolation
- Loss of money if a young person responds to a blackmailer's demands
- Nude images being shared non-consensually
- The levels of distress of young people in such a situation is clear and, in some cases, victims of sexual extortion have died by suicide as a result of their experiences,

Scenario

Mr Blake is asked to speak with a student in his year group who has been displaying unusual behaviour. Normally happy and engaged, Benji has been absent for most of the week and on return to school has seemed quiet and withdrawn. Benji reveals to Mr Blake that a girl he was chatting with online has revealed themselves as someone else and is now threatening to share nude images of Benji with all his friends, if he doesn't pay them £300. Benji has never taken a nude image but thinks the contact has created one using AI technology.

Risk across all 4 Cs

Online gaming

Gaming is extremely popular with children and young people. Games are easily accessible and can be played on various devices. Advances in augmented and virtual reality means that games can appear extremely realistic.

But with the increase in free gaming apps and live streaming, keeping children safe has become increasingly challenging.

Potential risks

Potential risks include:

- Being bullied.
- Trolling or being subject to scams.

- Costly in-game purchases. Children and young people may inadvertently spend large sums of money on apps or gaming websites.
- Talking to people they don't know and the associated risk of grooming.
- Being exposed to age-inappropriate material or chat.
- Oversharing through the voice and video technology used within games, including webcams and headphones or voice chat.

Scenario

George has started to use his dad's credit card for in-game payments to help him get a better football team with a nicer kit.

AI

AI stands for artificial intelligence, which is a type of computer program. It involves using machines and technology to complete tasks. AI systems are designed to complete tasks, answer questions and solve problems which previously would have required human thinking.

AI technology is increasingly sophisticated and can often be found as a feature in popular apps and services used by children and young people. AI is a tool and has many benefits when used effectively, however can lead to harm when misused.

Potential risks include:

- AI can be used to create realistic content including misinformation, scams, deepfakes or nude images, which may be difficult to identify as AI generated
- Young people may become overly reliant on AI tools; for example, for homework tasks, which restricts their learning and skill development
- Young people 'chatting' with AI; for example, chatbots, can develop unhealthy and parasocial relationships
- AI may collect data on its users, which can infringe children's rights, especially if used to encourage behaviour change or target advertising.

For further reading please see our Tes course 'Artificial Intelligence and Safeguarding: Understanding the Impact on Children'

Digital wellbeing

Digital wellbeing is about how the internet and technology can make us feel.

This includes recognising the impact being online can have on:

- our emotions
- mental health and wellbeing
- physical health and wellbeing.

As much as we try to build children and young people's resilience when faced with a difficult situation offline, the same should be done online. Children and young people should be encouraged to explore how to balance their lives online and offline. Technology and the internet should be there to enhance and simplify their lives rather than be a cause of distraction, worry or upset. Social media can be a great source of good, providing valuable connection even inspiration.

However, according to a 2023 report published by the U.S Department of health and human services:

'Usage of social media can become harmful depending on the amount of time children spend on the platforms, the type of content they consume or are otherwise exposed to, and the degree to which it disrupts activities that are essential for health like sleep and physical activity. Importantly, different children are affected by social media in different ways, including based on cultural, historical, and socio-economic factors.'

They go on to say,

'*social media use can be excessive and problematic for some children. Recent research shows that adolescents who spend more than three hours per day on social media face double the risk of experiencing poor mental health outcomes, such as symptoms of depression and anxiety; yet one 2021 survey of teenagers found that, on average, they spend 3.5 hours a day on social media. Social media may also perpetuate body dissatisfaction, disordered eating behaviours, social comparison, and low self-esteem, especially among adolescent girls'.*

A link to the report can be found in the **Resources** section.

A young person's digital wellbeing will be impacted by their online experiences from across the 4Cs. This is any negative online experience and may include:

- **Digital drama**
  Falling out and disagreements within friendships. The ambiguity of the internet and the fact that we cannot see someone's facial expression or hear their tone of voice can mean that messages and posts are misunderstood.

- **Desire to fit in**
  This could be pressure to look a certain way, lift self-esteem, receive a large number of likes or follows, or even pressure to watch and engage with content they may not be comfortable with.

- **Distressing content**
  Depending on the nature of what the child has seen, it can be difficult for them to reach out for help to understand what they have seen for fear of judgement or embarrassment.

- **Screen time**
  Managing the amount of time children and young people should spend online has been debated for many years. Watch the video, 'What is screen time? Young people give their thoughts', to hear the views of some children. A link can be found in the **Resources** section.

Finding the right balance becomes increasingly difficult as the child gets older.

Reflective task
Think about how much time you spend online. Now compare this to the screen time report reporting tool on your phone. How do they compare? How much time do you spend just scrolling?

Scenario

George will scroll through his social media for an hour before he goes to sleep.
George uses his computer to complete homework after school. He finds AI technology helpful to start projects rather than beginning from a blank page.

Longer time online means more potential exposure to the risks we have discussed throughout the module. It is crucial to remember and communicate to parents and carers that it is more about the quality of time spent online than quantity.

Children should be encouraged to have fun, engaging, and educational times using the internet rather than eliminating all chances for screen time whatsoever.

Parents, carers and professionals should also be aware that social media and the internet can be an important tool for children and young people to support their wellbeing. For some young people, internet use can be an invaluable way to access support, advice and community.

Summary

You have completed module one of your course on ‘Online Safety’, in which you have learned about your role in keeping children safe on the internet, why children and young people enjoy going online, and the 4Cs of potential online harm.

In the second module, we will consider how to prevent online harms and ways to respond to reports of online safeguarding concerns.

You are now ready to complete the corresponding questionnaire. Click **Questionnaire 1** to begin the questions.