Anstee Bridge

eSafety:

Keeping your child safe in a digital age

achieving for children

Introduction

The internet has changed the way we live. We use it for shopping, games, leisure, to keep in touch with friends and make new ones. We use it on computers, net books, laptops and phones.

Like everything, the internet has a downside. Reports of fraud and identity theft are common. However, the biggest worry for most people is the threat to children.

There are several ways in which children can be affected by things they do or see online.

- They may be exposed to adult material such as pornography.
- They may accidentally give away private family information like names and addresses.
- They may encounter adults who encourage them to do things that are not safe or legal.
- They may send photographs or messages which can be taken and used by other people.
- They may be the victim of bullies who use thinks like e mail or text messages to hurt and intimidate.

By following some simple ideas we can protect ourselves and make the internet a safe and fun place.

Social networking

Social networking platforms and app-based communication are a primary way for young people to stay in touch, share content, and express themselves. While traditional social networks remain active, platforms such as TikTok, Instagram, Snapchat, YouTube, and Discord are currently among the most widely used platforms by children and young people.

- TikTok, Instagram, and Snapchat (short-form video and photo sharing)
- YouTube and Twitch (video streaming and content creation)
- WhatsApp, Discord, and Telegram (group messaging and community servers)
- Roblox and online gaming platforms (interactive gaming with integrated chat features)

On all of these sites young people can invite others to become their ‘friend’. Once an invitation to be a friend has been accepted, then both people can see others' details.

Although younger children will enjoy other sites tailored to them, data shows they are also accessing the above platforms. These are slightly different social networking sites in that users create cartoon characters for themselves which can then interact with other characters on the site.

Instant messaging

Applications such as WhatsApp, Discord, Snapchat, and Instagram direct messages allow young people to communicate in real time through text, voice, and video. While convenient, direct messaging can expose children to unmoderated group chats, end-to-end encrypted messaging risks, and contact from unknown individuals if privacy settings are not properly configured.

Emails

All pupils in schools are provided with monitored school email accounts for educational purposes. Many young people also maintain personal accounts (such as Gmail or Outlook). It is important to ensure two-factor authentication (2FA) is enabled and personal credentials are never shared.

Using a mobile phone allows people to send text messages. These allow people who know the phone number to contact that person whenever the phone is switched on. Instant messaging can also be used on phones when they are connected to the internet.

The potential for harm

Bullying and cyber bullying

All of these facilities are available 24 hours a day and that is therefore possible for a bully to reach their victim whenever they like. Forms of electronic bullying can include:

- posting offensive or hurtful messages on a social networking site and encouraging other people to do the same
- sending abuse during instant message sessions
- creating a fake friend on social networking sites and encouraging the victim to enter a relationship and send messages which are then made public and mocked
- sending abuse via e mail or text messaging
- posting edited photographs

These are particularly harmful in that they reach the victim in his or her own home, where people generally feel safe. As so many people can view an internet page, the victim can feel exposed and humiliated.

Viruses, images and pop-ups

Digital threats include malware, phishing, and exposure to harmful or age-inappropriate content. Additionally, rapid advancements in generative AI bring specific challenges, including digitally manipulated imagery (such as deepfakes or non-consensual image creation), AI-generated misinformation, and algorithmic exposure to harmful material.

In accordance with Keeping children safe in education (KCSIE) guidelines and Achieving for Children (AfC) safeguarding protocols, proactive filtering and monitoring are essential.

Some website links may look innocent from their titles, but clicking on them brings up explicit images. Pop-ups are just that, little boxes which appear on the screen, often advertising sexual or other illegal services.

Online predators

There are several ways in which a predator can find and befriend potential victims. Most of them rely on the innocence of children and the anonymity of the internet which makes it easy for a predator to create a fake identity with which to fool victims.

Social networking sites are popular with predators as they can learn a great deal about a child just by reading his or her profile. For instance many young people display their full date of birth, helping anyone to work out how old they are. A predator can also learn a lot by looking at the friends and hobbies that they list. Check-ins can identify where their child is at any given time. An adult can then approach the child pretending to be another child, by claiming to be a similar age, background or to share an interest.

Webcams, smartphone cameras, and video calling applications (such as FaceTime, Zoom, or Teams) allow live video interaction. Once content or video streams are transmitted online, control over that media is lost, making it vulnerable to unauthorized recording or sharing.

Advice for parents and carers

Get to know the sites your child uses

'Think you know' website has lots of really useful and good information for parents and carers: www.thinkyouknow.co.uk. Click on the section marked 'Parent? Carer?' To find out more.

Understand the risks

The CEOP site is a great place to look for information on what can go wrong and how you can protect your child. www.CEOP.police.co.uk.

Invest in virus and pop-up protection on your home computer, most computer shops sell software that will protect your machine.

Make the internet part of your family. If possible have the computer where it can be accessed by everyone rather than in a child's room, this also makes it easier for a child to show an adult if something happens or scares them.

Webcams are brilliant tools, but should not be in a child's room they need to be in a public living area.

Know what to do if things go wrong

If your child encounters upsetting, abusive, or harmful online content (including cyberbullying, deep fakes, or grooming attempts), keep screenshots and evidence. In line with Keeping Children Safe in Education (KCSIE) standards and Achieving for Children safeguarding procedures, report concerns immediately to the school's designated safeguarding lead, the police, or via the CEOP Safety Centre.

You need to tell the child that you cannot keep the matter a secret and that you have to tell people who can help. Explain that this is to stop any other children being hurt.

If the problem is bullying messages sent by a classmate, you can take the matter up with school.

If the messages are either encouraging your child to meet someone or you are suspicious you can either report it to your local police or use the 'report abuse' section of the Child Exploitation and Online Protection Command (CEOP) website.

Use the internet safely

- Don't give away any personal or private information
- Information to keep secret:
  - full date of birth
  - your school
  - where you live, full address
  - email address
  - check your privacy settings
- Don't share your contact list
- Think about the photos you post
- Think about the messages you send
- If something happens that scares you or makes you feel worried or uncomfortable:
  - tell an adult you trust
  - report it on the CEOP website
- If you get friendly with someone online:
  - never arrange to meet them without an adult you trust with you
  - if they insist you go by yourself, something is wrong
  - trust your instincts
  - tell your friends about the risks too
- Spread the word

Further sources of help

Internet Watch Foundation (IWF): Confidential reporting of illegal online content. www.iwf.org.uk

CEOP: www.ceop.police.co.uk

Think You Know: www.thinkyouknow.co.uk

National Society for the Prevention of Cruelty to Children www.nspcc.org.uk

Childline: www.childline.org.uk

UK Safer Internet Centre: Online safety advice for parents, carers, and children: www.saferinternet.org.uk

Simple rules to tell your child to help keep your child safe

- Ask permission before using the internet.
- Only use websites you have chosen together or a child-friendly search engine.
- Only email people they know.
- Ask permission before opening an email sent by someone they don't know.
- Do not use chat rooms.
- Do not use their real names when using games on the internet.
- Never give out a home address, phone, mobile phone number.
- Never tell someone where they go to school.
- Never agree to meet someone they have met on the internet.
- Only use a web cam in a public area.
- Tell you immediately if they see anything they are unhappy with, feel scared about or makes them feel uncomfortable.