NSPCC

Cruelty to children must stop. FULL STOP.

The information in this guide has been taken and adapted from the NSPCC website. You can find more information on online safety for children at NSPCC.org.uk

Keeping Children Safe Online

A short guide on ways you can protect your child from online harm. Includes information on:

- Protecting from online abuse
- Livestreaming
- Online gaming
- Parental controls
- Talking to your child about online use

www.barnardos.org.uk

www.facebook.com/BarnardosNI / @BarnardosNI

Barnardo's Registered Charity Nos: 216250 and SC037605

The Jigsaw PROJECT

Believe in children

Barnardo's Northern Ireland

Protecting children from online abuse

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- be withdrawn, upset or outraged after using the internet or texting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: the 3Cs

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

Livestreaming

Livestreaming is broadcasting to an audience in 'real time'. The audience can leave comments, give likes to the person who is streaming and, in some cases, 'gift' the streamer. Some platforms let several people livestream at the same time.

Risks of hosting a livestream	Risks of watching a livestream
• Feeling pressured • Feeling less inhibited online • Talking to strangers online • Bullying comments • Videos being recorded or shared without consent	• Seeing inappropriate or upsetting content • Inappropriate or upsetting comments

What are the main livestreaming platforms?

Twitch (13+)	Yubo (13+)	Bigo (18+)	Monkey (18+)	Omegle (13+)	Clash (13+)	Facebook (13+)	Instagram (13+)	Tiktok (13+)

Understanding Online Games

Online games can be a great way for children and young people to keep busy and stay in touch with friends and family, but it's important that they play safely.

Things to consider if your child games online:

- **age ratings of games they play**
  - Most games have an age rating based on their themes, those with violent and sexual content will have a higher rating. The age rating system is provided by PEGI and gives an overview of individual games which can help you to decide if it's appropriate. For example, Fortnite is rated age 12+. *These ratings don't include communication features, so a game with a low age rating may let children speak to people they don't know.*
- **messaging and contact functions on the games**
  - Some games let players turn off communications features, mute voice chat and report other players who behave inappropriately. Look at the settings available to see what's best for your child. All major games consoles have settings that prevent children from finding inappropriate games. You can set limits on how long a young person can play and prevent them from speaking to unknown players. It's a good idea to explore these settings before your child plays the game.
- **in-game purchases**
- **trolling, "griefing" and scams**
- **how to report problems**

Also, if you have more than one child in your home, be aware that games suitable for one child to play or watch, may not be suitable for another.

Deciding if a game is appropriate

There are four main things that you can consider to help you decide if a game's appropriate for your child to play:

Check the content of the game and any chat function:

- Content within games is regulated and rated into age groups based on elements within the game such as sex, violence, gambling, drugs, in-app purchases etc. There are lots of different age ratings around the world, such as PEGI used in the UK. Always check the age rating to help you decide to allow your child to download or play a game - this is normally visible next to the game title within gaming and app stores.

Consider who your child could have contact with whilst using the game:

- Consider any communication channels and if there are settings to turn off or limit chat functions. There can be different types of communications, e.g. group chat or private chat.
- Communication in a game can increase the risk of bullying (sometimes referred to as being 'griefed' within gaming), being contacted by people they don't know and potentially groomed or exploited. Many games have a means of communication which includes private messaging and private chat. Look out for words like 'whisper' or 'private' next to messages if your child is playing in multiplayer games (especially if they are playing with people they don't know offline) and any suggestion of taking the conversation to other messaging platforms.

Does the game have in-app purchasing?

- In-app purchases normally enhance the game or gameplay, for example skins (design of the character or weapon) or loot boxes (treasure chests, but you don't always know what is in them). There can often be considerable pressure on children to be unique within their games (new skins) or to be better than others (purchasing power-ups). You should consider settings to turn off in-app purchases, or set a spending limit on the device or app.
- Children need to be aware of scams involving free in-game currency (e.g. V-Bucks in Fortnite, or Robux in Roblox). Scam text messages, forum posts and videos may have content advertising free in-game currency. But they're often scams, designed to coax the player into revealing their gamer tag (username) and password in return for currency. This is known as a 'phishing' scam.

Does the game affect your child's behaviour?

- The behaviour of your child could be affected by some games, it can include bullying or 'griefing' others, trolling or other inappropriate behaviour. Very intensive games can result in short-term bad behaviour such as poor temper or 'ragequitting', which is getting so upset they stop playing immediately. Ensuring a game's suitability can help, as can limiting playing time.

Parental Controls

The limits of parental controls

Whilst parental controls are a helpful tool there are limitations. So they shouldn't be seen as a whole solution; parental controls are just part of the way you can help keep your child safe online.

More top tips include:

- Talking to your child. Explain why you are setting parental controls; to keep them safe. But also let them know that they can talk to you to discuss why certain settings are in place.
- Set good, strong passwords where you are able. On some parental controls you can set a password which prevents settings and features from being changed.
- Age is a significant factor; as children get older, restrictions and controls you use will change, but only at a pace that is appropriate for your child, not pressure from your child "because everyone else is allowed".
- Content filters are never 100% effective, it is likely at some point that your child will see inappropriate or upsetting content and it is important that you are able to talk to them about this.

Setting up parental controls on:

Home Broadband and Wifi

Home internet providers can offer parental controls for your family. You can:

- use a filter from your internet provider to control the content that you and your family see. Some providers allow different settings for each user.
- set up any device connected to your home broadband. How you do this depends on your provider and you'll need to access your home router. You can ask your internet provider for help setting this up.

Games Consoles

Most games consoles have internet access, which means your child can go online and chat with other players or make in-game purchases. On many consoles there are parental controls which allow you to manage which features are available to your child.

On some devices you can:

- turn off chat functions to stop your child from talking to people they don't know
- restrict games based on age
- turn off in-game purchases, or set a limit.
- Check the website for the console your child has for a parents section and details of features.

PlayStation Family Management: On PlayStation consoles you can set up a Family Manager account which allows you to manage different accounts for different children/users. Within this you can manage a range of features, such as restricting communication with other players, restricting content, setting play time controls and set spending limits.

WiFi and Being Away from Home

The controls you've set up on your child's device and your home broadband won't work if they use 3G or 4G, public WiFi or log onto a friend's connection instead. Remember:

- public WiFi is often available when you're out and about, but it's not always safe
- some public places and businesses offer family-friendly WiFi. When you see the family-friendly WiFi symbol it means there are filters to stop children from seeing inappropriate or upsetting content
- talk with your child and agree what they can and can't do online. If your child is visiting friends or family, remember that they might not have the same controls set up.

Search Engines

Sometimes, innocent searches can lead to not so innocent results. If you're worried:

- make sure the content your child sees online is appropriate for their age by using parental controls and filters in search engines like Google, Yahoo and Bing
- make sure you have set parental controls on the home broadband and devices.

Google Family Link - a very useful app to manage a range of features such as restricting content, approving or disapproving apps, setting screen time and more. For lots of useful information see the Google FAQ page.

Mobiles, Tablets and Computers

All mobiles, tablets and computers have parental control settings, which can differ between devices, these include:

- allowing or disallowing in-game or in-app purchases
- settings such as location settings and what information your child is sharing
- wellbeing settings to help with limiting screen time.

You can get more advice about setting up controls on different devices from your mobile provider and the UK Safer Internet Centre. On Apple devices such as iPhone, iPad, Apple Watch, Apple TV etc. there are features available for parents all tied into an account. You can set content and privacy restrictions, prevent purchases, allow or disallow apps and more.

Apps and Online Services

Many social media, apps and online services such as streaming services have features such as:

- content filters
- chat filters
- privacy settings
- in-app purchase settings.

You can find out about these features by looking in the settings on each app, or take a look at their website for more information. They might be called settings, family features, privacy or security.

Facebook has a Parents portal which helps explain the features available. For Netflix, you need to visit the website to set up parental controls – we suggest you do this as soon as you create an account.

Microsoft Family Safety – by creating a family group you can manage many settings, such as setting screen time limits, blocking inappropriate content, set game limits and more. To learn more see the Microsoft page and Xbox Family Settings.

Talking to Your Child

Technology can move at an extraordinarily fast pace and it can be difficult to know how to start talking to your child about what they're doing online, who they might be speaking to or discussing the potential risks and issues.

Starting The Conversation

Talking regularly with your child is the greatest tool to help keep them safe online. Talking regularly and making it part of daily conversation, like you would about their day at school, will help your child feel relaxed. It also means when they do have any worries, they're more likely to come and speak to you. But it can also be easy to become overwhelmed with the different technology, the language that children use, the huge number of games and apps which are available and the potential risks.

Age-Appropriate Conversation

A big factor to consider when we're talking to children is age or cognitive ability, which also impacts on the language we use and what we can talk about.

As children get older, their needs and behaviour will change, particularly as children are moving through their teenage years and are more prone to risk-taking, mood swings or whether they will even talk to you about something that they may be embarrassed or ashamed about.

For example if you suspect grooming or exploitation, you may not wish to talk about this directly with a younger child, but instead report directly to CEOP. But you can also use resources such as PANTS to help with the conversation.

With an older teenager you may be more comfortable talking about these issues. There are some tips in our Positive Parenting guide and our page on talking about difficult topics which you may find useful.

Tackling Difficult Conversations

Some conversations are going to be more difficult than others, but it's so important to have these open and honest conversations, so you can help your child with any worries or issues they might be facing online. For example, if you're worried they have been viewing online pornography, if they have been sharing nudes, if they have seen upsetting, inappropriate or explicit content, or perhaps being bullied. These more difficult conversations will heighten feelings of fear, anxiety, worry, shame and embarrassment.

As with any conversation, it is important that we try to stay calm, balanced and non-judgemental.

- If it's something that has made you angry, fearful or concerned, don't tackle it straight away if possible. Those feelings will affect the way we talk. Take a little time and, if possible, talk to someone else about it. Your child's school can be a great source of information, particularly the class teacher and the Designated Safeguarding Lead.
- Don't be too forceful otherwise there is the risk that they will close down.
- Consider a subtle approach instead of a head-on approach. For example, you could ask if the subject is discussed at school and what they learn about it, or it could be something that has been on the TV or you heard about it on the radio.
- Keep listening, try not to interrupt even if there is a period of silence. They may be thinking how they word something.
- Provide context. Allow them to understand why some things are wrong, age inappropriate or even illegal. In order to critically think and assess, they need information.
- Remind them of your family values; some parents may think that something is okay for their children, but explain why you don't think it is appropriate for your children.
- Children often talk of being punished. For example, if they open up to you and say that they have seen explicit content by accident, they are fearful of their devices being removed from them. This is seen as a punishment and consequence for something that was out of their control. This is a judgement call that needs to be carefully handled.

Summary

Children at any age need to be kept safe online. This can be overwhelming however the three main areas to focus on being aware of content your child sees, who they contact, and how they behave online.

A sign of concern is a child's behaviour towards technology changing. This could be either using it more or using it less than usual, or being secretive about how they are using it

Livestreams can be a risk to watch or participate in and most livestreaming sites are either 13+ or 18+. Be sure to check if the apps or games your child is using have livestreaming functions.

Online gaming:

- age ratings are very important and should be followed to protect your child
- in-app purchasing risks are real, ensure your child or device do not have access to your bank details
- chat functions are on most games, be sure to check what they are for each game, who can contact your child and how

Parental controls can be set up on individual devices or on WiFi networks

Controls are not a replacement for communication. Most important thing you can do is talk regularly with your child about their technology use. It is important to do this from an early age, and use it as a preventative measure to keep your child safe rather than a response to something happening