



On-line Safety

Parental/carer Information

Deciding what's appropriate for
children to see online



What is appropriate for your child?

The online world gives us access to a huge amount of information and services, but the scale of information available also means that there is content that is inappropriate for children. What is or isn't appropriate is up to individual parents and carers to decide, and could be based on things like age, ability, beliefs and family values



What are Parental Controls?

- Parental controls allow you to block and filter upsetting or inappropriate content. They work across your WiFi, phone network, individual apps and devices.



Parental Controls

- Parental controls can help you to:
- plan what time of day your child can go online and how long for
- create content filters to block apps that may have [inappropriate content](#)
- manage the content different family members can see.

Inappropriate or explicit content

- Edited or filtered images and videos
- Many platforms now have in-app filters or editing tools to help you alter an image or video. Some filters can be used for fun, to add silly props or masks to an image or video.

Edited or Filtered Images

- However, when filters or tools are used to enhance or alter physical features, this can lead young people to compare themselves to others online and have an unrealistic view of acceptable beauty standards. It's not always easy to recognise when someone is using a filter, for example there are tools available that enable you to edit your appearance.

Impact of Filtering

- They can affect young people's self-esteem and body image.
- Young people may feel pressure to post certain images to 'fit in'.
- They can affect young people's overall wellbeing.
- Young people may feel disappointment or embarrassment if they don't get enough 'likes' or comments.

Fake News, Hoaxes and Misinformation

- Digital platforms have made it easier for anyone to share information online, and it can be difficult to determine whether something is real or false.
- What a young person sees online can shape how they view the world and impact their overall wellbeing. It's important to talk to them about how misinformation spreads and how to look out for it.

Misinformation & Disinformation

- **Misinformation** is where false information is shared by accident without the intent to cause harm. For example, sharing inaccurate photos, quotes or dates online because you believe them to be true.
- **Disinformation** is false information shared deliberately to mislead and cause harm. For example, fabricated news stories and political propaganda



What is real & what is false?

- Digital platforms have made it easier for anyone to share information online, and it can be difficult to determine whether something is real or false.
- What a young person sees online can shape how they view the world and impact their overall wellbeing

Video

<https://www.youtube.com/watch?v=ySbDYUmPasU>



Examples - Hoaxes

- **Fabricated or false news stories** about current news that might make a child feel worried or scared about what's happening in the world. This is commonly known as 'fake news'.
- **Mememes** can be used to spread unverified facts.

Hoaxes

- **Viral messages** containing false information can easily be shared on messaging apps like WhatsApp and Messenger. If you or your child know the person who has shared it, you might be more likely to believe it.
- **Deep fakes** are videos where people's faces are edited to make it look like they said or did something they didn't.

Scams

- An online scam is where criminals use online platforms to trick someone into sharing personal information like account logins or bank details. Scams can happen on any online platform

Scams

- **Phishing emails or messages** sent to a personal device asking you to provide personal information or contain blackmail demands. Sometimes these will be made to look like they're from credible organisations or businesses.
- **Promotion of products or false adverts that contain untrue claims.** For example a fake competition or a product that claims to do something it can't to encourage others to purchase it.

Scams

- **Catfishing** where some will pretend to be someone else to trick them into doing something.
- **Competitions or quizzes** where you are led to believe there is a prize.
- **Identity theft** where people are tricked into sharing personal information to help them hack other accounts.

Online Challenges

- An online challenge is an online activity that normally involves sharing an image or video of yourself doing a set task. They can take place on most online platforms but are most commonly on video sharing platforms like Tik Tok or YouTube

On-line Challenges

- Some online challenges can be fun for young people to participate in. For example, challenges that involve dancing or those that help raise money for charity. However, online challenges can become risky when they contain dangerous stunts or activities that could cause physical or psychological harm to a young person

SETTING UP PARENTAL CONTROLS



Home Broadband & 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

Home Broadband & WiFi

- 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. Remember that this only affects your child accessing the internet through the WiFi – if they are using 4G or 5G etc to connect you need to check the settings on their mobile device too.

<https://www.youtube.com/watch?v=ZaSjHFhOI-0>

<https://youtu.be/sz4EyUMUTro>

<https://www.youtube.com/watch?v=sz4EyUMUTro>



Game 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:

Game Consoles

- 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.

Game Consoles

- Check the website for the console your child has for a parents section and details of features. Some games also allow you to change settings for that individual game.

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. See all the features available for [PS4](#) and for [PS5](#).



Mobile, tablets & 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.

Apple Devices

- 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 film and TV streaming services have features such as:
 - content filters
 - chat filters
 - privacy settings
 - in-app purchase settings.

Apps and Online Services

- 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.

Apps and Online Services

- **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.

Apps and Online Services

- **Microsoft Family Safety** – by creating a family group you can manage many settings, such as setting screen time limits, blocking inappropriate content, receive activity reports, set app and game limits and more. To learn more about Microsoft Family Safety see the [Microsoft page](#) and [Xbox Family Settings](#).



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.

Search Engines

- [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](#)

Video 1

<https://www.youtube.com/watch?v=ZaSJHFhOI-0>



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:



WiFi and being away from home

- 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

WiFi and being away from home

- 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.

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. Even if you've put things in place on your home broadband and your child's device, they won't help if your child connects to a different WiFi with no controls in place.
- Parental controls are just part of the way you can help keep your child safe online



MORE TOP TIPS



Top Tips

- 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.

Top Tips

- 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

Nicholas Postgate Catholic Academy Trust is committed to quality of opportunity, safeguarding and promoting the welfare of children, young people and vulnerable adults and expects all staff and volunteers to share this commitment.





<https://www.youtube.com/watch?v=sz4EyUMUTro>



















