Online Safety

Benefits of using devices

- Communication

- Enjoyment and entertainment

- Developing skills and knowledge

General risks of being online

Contact with Others
Often, online games have the option to connect with other users. Without the right settings internet users who your child has not met can contact them.

Requests for Personal Information
These could come from real people, in the form of emails or messages, or through phishing. The word phishing describes a person or group of people who try to scam you by sending emails or creating web pages that look real. It is a cyber-attack where cybercriminals try to gain sensitive information from you by pretending to be someone you would normally trust.

Requests for Money
Sometimes, applications or games require payment information before you can play. If this is stored in the game, it can be all too easy to accidentally authorise a payment in the middle of a game. It is not always clear to children whether it is real money or an in-game currency that they are spending. Requests for money can appear on websites or in messages and emails too.

Computer Viruses
These are pieces of code that can copy themselves. This can result in your computer or other system becoming unusable. Viruses can destroy data too.

Online Risks for our pupils

Research shows that the age at which children are accessing smart devices and the Internet is getting younger and younger. There are also studies that show that autistic people and people with disabilities are more at risk online than those who are not disabled or not autistic.

Social Awareness

Understanding of risks

Compulsive tendencies

Self-regulation

Why Is Online Safety Important?

It is never too soon to start good online safety habits with your child.

Just as you would want to protect your child from harm in the real world, it is vital to do the same in the digital one. It is important to give children the skills they will need to explore and engage with the digital world in a positive way.

Technology and the way in which we interact with it has a vast impact on both our mental and physical health so we need to think carefully about:

- screen time
- interacting with others online
- online content
- privacy and security

Family Agreement

Consider:

Where they use their device

When?

How long for?

What are they accessing

Who is available to help?

Family Agreement

Use my tablet in the living room

Parent will give me 10 + and 5 minute warning

before it's time to finish

I will use my timer while i use my tablet

Screen Time

Monitoring Screen Time

Children often do not realise how long they have been online so why not get them to use a timer to check how long they are spending in front of a screen each day? It might be useful to set a screen limit. You could discuss this together and create a timetable or use a timer to help them stick to the time limits.

Including TV 1- 3 hours is often how long children and young people spend on screens.

Generally it is advised avoid screens while eating, an hour before bed and in bedrooms.

Regular Breaks

Sometimes, your child might need a reminder to step away from the screen. You can prompt them to stand up, change position and gently stretch their muscles. You could also go for a walk for a change of scene too.

Screen Time

Stretch It Out
Making plans to do activities with friends or family that do not involve a screen can help us all see the benefit of other activities. Alternatively, your child could join a club or take up a hobby based on one of their other interests.

Screens off Overnight
It is useful to encourage your child to turn their screens off an hour before bed. You may choose to keep devices in another room at night.

Device Settings
You can show your child how to use 'do not disturb mode' on their device so that they can focus on other things. There are also options such as changing colour settings to help reduce eye strain.
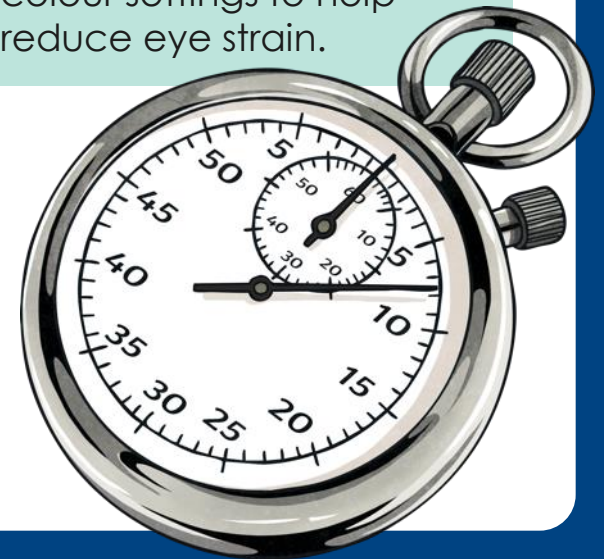
Interacting with Others Online

Ideally if children are gaming – switch to a mode such as friends only, invite only, party play

It is important to create a culture of openness in order to make sure they are interacting safely. Here are three ways to do this:

- Check in regularly with your child about their contacts
- Be aware of who else is involved and make sure that your child is only talking to people they know in the real world.
- Ask them to show you some of their conversations so you can get a feel for what is going on in the chats.

Teach your child to be kind and respectful to others online and to expect the same treatment in return. Games and websites often have the option to block or report users and this is definitely worth investigating if your child has seen or heard something online that has upset them.

Online Content

Shielding your child from inappropriate online content is a high priority.

One way to do this is to set up filters or parental controls on devices.

You can also encourage your child to use child-friendly search engines, such as Swiggle or DuckDuckGo, and discuss the importance of reporting anything that makes them uncomfortable. Younger children should stop what they are doing, close or switch off their device and then tell a trusted adult what has happened. Older children should be encouraged to report what has happened via the app or website they are on, save evidence such as screenshots and block the person or people responsible.

Even with the best filters in place, children are still likely to come across inappropriate material occasionally. Talking openly with your child about this and setting simple rules for what to do is an important way to build your child's digital resilience.

PEGI Ratings

The age ratings for green PEGI 3 and PEGI 7 games are advisory.
The age ratings for the orange PEGI 12 and PEGI 16, as well as the red PEGI 18, are legally enforceable. This means that shops cannot sell or hire games with an orange or red rating to people who are not the right age.
Online and downloaded games are not technically included but many major providers voluntarily add the limits to their games.

3 PEGI 3 — Suitable for all age groups. These games should not include any sounds or pictures which will frighten young children. There should be no bad language. Mild forms of violence can only be used in a comical or childlike setting.

7 PEGI 7 — Games may contain scenes or sounds that could frighten young children. They can also contain mild forms of violence but this must not look realistic and must not be too detailed.

12 PEGI 12 — Games may show violence in a slightly more graphic way towards fantasy characters. Violence towards human-like characters is still unrealistic. There may be gambling and suggestive activities or language included. Bad language must be mild.

16 PEGI 16 — Games can feature more realistic violence. Games may include tobacco, alcohol or illegal drugs and stronger bad language.

18 PEGI 18 — This is an adult classification. These games can show all of the content from the PEGI 16 rating but also contain realistic and extreme violence, as well as other events that are only suitable for adults.

Parental Controls

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 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](#)
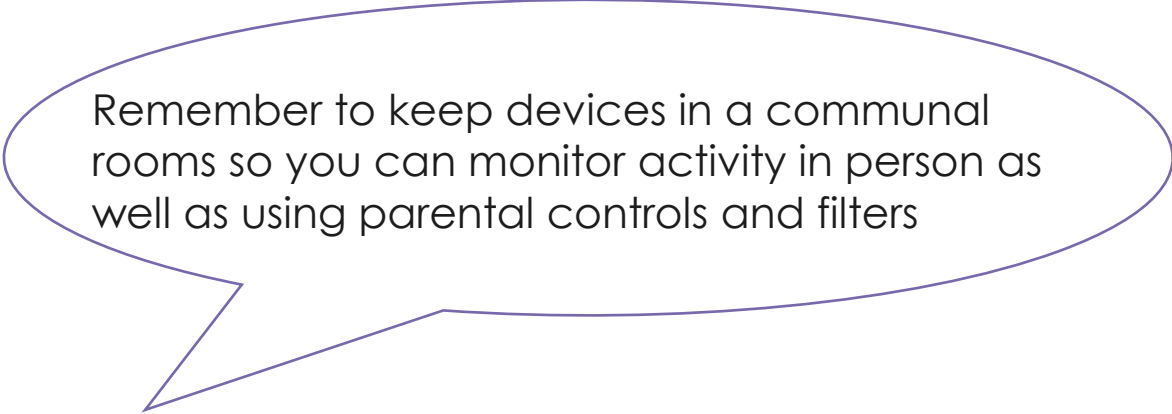
• Manage the content different family members can see.

Safer searches

Child friendly browsers:

Google Safe search for kids

Google Family Safety Centre

Yahoo search safety guide

Remember to keep devices in a communal rooms so you can monitor activity in person as well as using parental controls and filters