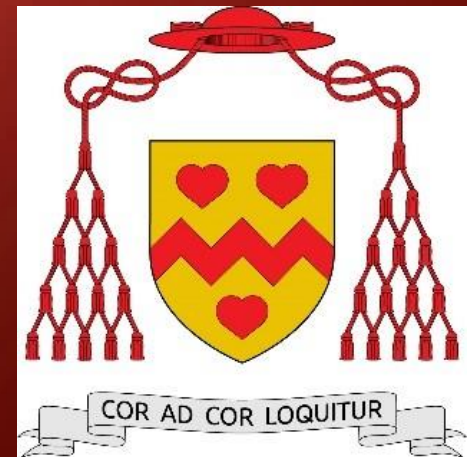


# ST JOHN HENRY NEWMAN CATHOLIC SCHOOL ESAFETY NEWSLETTER

WINTER 2022



# UNDERSTANDING ONLINE GAMES - 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.

# UNDERSTANDING ONLINE GAMES - DECIDING IF A GAME IS APPROPRIATE

## **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.

## **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



# SMARTPHONES

Many people are glued to their phones these days, but is there anything that should concern you about this?



## Camera care!

The camera. Don't take photos of people or share them without that person's permission. Turn off geotagging too to avoid people finding your location.



## Sleepless nights?

Sleepless night? Turn off your phone an hour before bed. Your phone's bright screen stops the brain to stop producing "time to sleep" cues.



## Turn off notifications

Turn off notifications from social media and games. Reducing time spent looking at your phone is healthy, but if it is beeping and vibrating at you this is hard!



## Keep active!

The technology revolution has led to reduced physical activity and a range of health issues. Put down your phone and do some exercise!

# ANONYMOUS APPS

Anonymous apps allow users to share and interact with each other without revealing who they are. Unlike social media sites, many of these apps encourage users to stay anonymous and chat to each other or post questions and answers on a range of topics.

Although anything shared on these apps is anonymous, it's important to note that anonymity is not guaranteed as certain types of information like an IP address or cookies can be used to identify who you are. Also, some apps sync to a users contact list or location to provide a personalised experience on the platform.

The ability to be anonymous and ask questions that may be sensitive or embarrassing is one reason why millions of teens worldwide are using these apps.





# ANONYMOUS APPS

These apps remove the anxiety of presenting your 'best-self' online and allow teens take on different personas and explore different ideas without fear of repercussions.

Anonymous apps can expose children to a range of online risks, including inappropriate content, cyberbullying and sexting.

Under the cover of anonymity, people may feel less accountable for what they say and may share things that they would not on open social platforms.

By the very nature of these apps, keeping teens safe becomes that much more of a challenge, so having a regular conversation on the subject is key

# ANONYMOUS APPS



Check age ratings of any apps you're not familiar with. It's a good idea to use app store settings to only show age-appropriate apps. Also, review the privacy settings on these apps to make sure they are in control of how their information is used, who can see their account and what they share.

Children seek out norms to follow so it's important to sit together and set some boundaries on the types of apps they can and can't download. This will help them understand your concerns and why it is beneficial for them to use certain apps and not others.

# ANONYMOUS APPS

Although anonymous apps may hide your identity to some extent there are certain pieces of information that can identify you like an IP address so it's important to advise children not to say or share something they wouldn't want to be shared publicly.

If your child is being cyberbullied then be calm and considered, listen to their concerns and offer your parental support. Don't deal with it alone, talk to friends and contact school and ask about our anti-bullying policy.



# LEARNING FOCUS THIS TERM

On our return to school this term, our Key Stage 3 pupils have revisited online safety looking at a range of topics including their digital footprint, the concept of live streaming and sharing inappropriate images online. In all cases we have discussed the importance of the report button where students feel upset, shocked, or uncomfortable with anything they see online. Most websites have a report button or students can visit the CEOP to report their concerns there. Our own school website contains a [report button](#) where students can alert us to any worries, they may have over online bullying.

It has been surprising how many of our year 8 students were able to name and describe what different live streamers do. It is becoming ever more popular; it has become so cheap and easy to buy a ring light to ensure even lighting and cast out shadows on those all-important close ups. This [link](#) provides advice on key messages for those who may wish to live stream or who want to watch a live stream. Our Year 9 students have been discussing the issues around the sharing of images, those that might be considered inappropriate. Our discussions focussed on why an individual may feel compelled to send an image and the consequences this can lead to. When asked, all students were able to identify scenarios that would be breaking the law. Further advice can be found [here](#).

# Did you buy gaming console this Christmas?

All consoles offer additional parental controls to limit time spent on the device or limit who your child can communicate with online. Also, be aware of the PEGI ratings on a game which shows you the age suitability of the game e.g. a PEGI rating of 12 shows the game is only suitable for players over the age of 12 due to its content.



## Xbox Series X|S and Xbox One

Xbox offers built in family settings to help you manage the following:

- Set screen time
- Filter content based on your child's age.
- Limit who your child can communicate with online.
- Approve your child's purchases.
- Set up "Ask a parent" for your child to add a friend.

Find out more here: <https://www.xbox.com/en-GB/community/for-everyone/responsible-gaming>



## Nintendo Switch

The Nintendo Switch Parental Controls smart device app is a free app that can be linked with Nintendo Switch to monitor what your child is playing. The app creates a report so you can see which video games your child plays and how long for. It also allows you to set which games your child can play based on their PEGI age rating and restrict your child from sending/receiving messages from other users.

Find out more here: <https://www.nintendo.co.uk/Nintendo-Switch/Nintendo-Switch-Parental-Controls/Nintendo-Switch-Parental-Controls-1183145.html>



## PS4

PS4 offers a variety of Parental Control/ Family Management options such as:

- A System Restriction Passcode - stops other users from logging into your account to make changes to your parental control settings.
- Restrict Age Level for Games (based on PEGI ratings)
- Restrict Blu-ray discs and DVD movies
- Restrict use of PlayStation® VR - this is not for use by children under 12 years.
- Disable the Internet Browser.
- Disable children from communicating via chat, messages, or displaying and entering comments for friend requests and game invitations.
- Hide games and game features based on your child's age.
- Set the monthly maximum amount of money a child can spend in the store.

Find out more here: <https://support.playstation.com/s/article/PS4-Parental-Controls>



## PS5

As with PS4, PS5 includes parental controls and spending limits to help you manage your child's activity. You will need your own account for the PlayStation Network and an account for each child. There are preset parental controls in three categories - Child, Early teens or Late Teens.

You will be able to:

- Set age rating levels for games and apps.
- Restrict Blu-ray discs and DVD movies
- Restrict use of PlayStation VR.
- Restrict web browsing.
- Restrict communication.
- Set the monthly maximum amount of money a child can spend in the store.

Find out more here: <https://www.playstation.com/en-gb/support/account/ps5-parental-controls-spending-limits/>



# CHANGES TO PARENTAL CONTROLS ON TIKTOK

Following continued coverage of the risks the platform can pose to children and young people, TikTok has announced changes to its parental control settings. This article details the changes to the parental control settings and provides an overview of existing settings you can use to protect the children in your care.

**The following new features mean that parents can now:**

- Restrict who can view their child's profile and comment on their posts
- View what videos their child has liked
- Control what their child searches for including hashtags, videos, user profiles and sounds

**Existing TikTok features already allow parents to:**

- Set a time limit on their child's screen time
- Limit content that isn't suitable for their child
- Manage their child's privacy and safety settings
- Choose whether their child's account is private or public



## Childline Report Remove tool

Childline has launched Report Remove, a service that allows children and young people under 18 to report and get removed from the internet a nude image or video of themselves that might have been shared online. This can be accessed at

<https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/remove-nude-image-shared-online/>



# GLOSSARY

- **Anti Spam** Computer program that puts into action anti-spam/spim/spit techniques
- **Anti Virus** Software Application designed to protect PCs from malicious computer code (virus)
- **AUP Acceptable Use Policy** - set of rules applied to a network, website or computer system that restricts the ways the network site or system may be used. Most schools and businesses use them.
- **CEOP** Child Exploitation and Online Protection dedicated to eradicating the sexual abuse of children. Part of UK policing tracking and bringing offenders to account. [www.ceop.gov.uk](http://www.ceop.gov.uk)
- **Encryption** The science of scrambling data be it text, audio, or video so that it can only be read by the authorised sender and recipient.
- **Cookie** A small piece of data sent from a website and stored in a user's web browser while a user is browsing a website.
- **Cloud Computing** Storing and accessing data and programs over the Internet instead of from your computer's hard drive.
- **File Sharing** A system in which users write to as well as read files or in which users are allotted some amount of space for personal files on a common server, giving access to other users as they see fit.
- **Filtering** Software or hardware product designed to prevent access to inappropriate websites on the internet. It does this by denying or allowing access based on lists of pre-classified addresses, or by examining the web data for keywords or unwanted content.
- **Firewall** A system that prevents unauthorised access to a computer over a network, such as the internet. Firewalls can be either hardware or software businesses tend to use the former; home users the latter.

# USEFUL LINKS

<https://nationalonlinesafety.com/guides>

<https://www.thinkuknow.co.uk/>

<https://www.internetmatters.org/advice/>

<https://www.nspcc.org.uk/keeping-children-safe/online-safety/>

Or contact us at school if you have any questions