



VMAT

Online Safety News

Issue 4

November 2019

Contents

Page

3	Introduction
4	New Devices for Christmas
5	Games and Apps, Smart Toys
6	Where Can I Go for Online Safety Help?
7	Digital Wellbeing
8	Privacy Settings & Parental Controls
10	Social Media and Sharing Information
12	PEGI Ratings





This booklet is a basic guide to helping keep you and your children safe online.

The internet is constantly evolving, changing and adapting which means that this information can quickly become outdated.



The main steps you need to take are:

1. Talk to your child about what they are doing online, ensure that they know they can always speak to an adult if something goes wrong.
2. Keep all your privacy settings updated and check them regularly.
3. Be mindful of what you and your child are sharing and who it is shared with.

Remember, once something is online it will be online forever.



There are lots of great websites you can use for further advice.

www.thinkuknow.co.uk/parents/

parentzone.org.uk

www.commonsensemedia.org

www.childnet.com

www.saferinternet.org.uk/



New Devices for Christmas



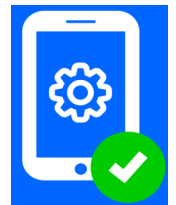
Over Christmas many children receive gifts that require going online (smartphones, gaming devices, tablets, etc). We have compiled a short checklist to help keep your children as safe as possible whilst using their new devices.

1. **Research the device**, make sure you have an idea of how your child will be using it.

www.saferinternet.org.uk/advice-centre/parents-and-carers/parents-guide-technology is a very helpful website which provides information about different devices (smartphones, tablets etc.)



2. **Set up security and parental controls before Christmas Day**, paying special attention to location settings. If you can't set it up before Christmas ensure you sit with your child and set it up together. pwxp5srs168nsac2n3fnjyaa-wpengine.netdna-ssl.com/wp-content/uploads/2018/01/IM-SetUpSafe-Checklist-24Jan.pdf this is a helpful checklist.



3. **Look into the parental controls on your home internet.** <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/parental-controls-offered-your-home-internet-provider> this website provides helpful information on different service providers. For smart phones check parental controls are also set up on the mobile network .
4. **Play on the new device together with your child**, talk about what the child is using it for and what they know about staying safe online.





Games and Apps



Along with new devices, children will also be receiving new games and downloading new apps. Some of these will not be appropriate for your child. There are several ways that you can check the games/apps to ensure your child isn't exposed to inappropriate content.

1. Look at the PEGI rating. This is an age rating used for games and apps, it will also give an indication of the type of content the game has.
2. Check the game/app on www.commonsensemedia.org/ this is a great source of information about games and apps and what to expect from them.
3. Play the game yourself, this is a great way for you to experience the game and any issues your child might encounter.
4. Use YouTube to watch videos of the games/apps being played.
5. Spend time with your child while they're playing the game and see for yourself what they are seeing. Ensure all chat functions are turned off.



Smart Toys (Internet Connected Toys)

In recent years new smart toys have been developed that access the internet, this might mean that the toy collects data and could possibly be accessed by other people.

It is important to research the toy and find out about:

- The type of information the toy collects
- Will it take photos or videos and where they are stored?
- If it uses location services
- Who can interact with the toy and does it require a password?
- Are there parental controls?



<https://parentzone.org.uk/article/12-ways-make-connected-smart-toys-safer>



provides helpful information on setting up your smart toy, for example turning off location services and changing any default passwords or pins.

Where can I go for Online Safety help?

If you have an online safety incident the first thing you need to do is REPORT it to the website or app that it happened on.



The reporting option is normally found in either a cog icon 

3 dots  or 3 lines 

You can also report it to CEOP this is the Child Exploitation and Online Protection command. They deal with any communication with children online that you are suspicious or worried about. <https://www.ceop.police.uk/safety-centre/>



If the incident is a form of bullying then visit the Childline website, where you can make a report and seek advice. <https://www.childline.org.uk/>

You can ask in school for further advice. Mr Harvey and Mrs Tully are happy to help if needed. The school website also has an online safety page with helpful information.

<http://www.trevithick.cornwall.sch.uk/children/online-safety/>

Other helpful websites are:

Common Sense Media - this website provides reviews about games, films and YouTubers. You can read what to expect and decide whether you think it is appropriate for your child.

<https://www.common sensemedia.org/>



ThinkUKnow - this website provides lots of guides for keeping your children safe online. As well as providing advice for making a report.

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



Internet Matters - This website provides easy to follow help sheets for setting up privacy settings and parental controls. As well as further advice on Online Safety and screen time.

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



ParentZone - This website provides information on the latest Online Safety Issues as well as guidance and advice.

<https://parentzone.org.uk/>



Digital Wellbeing

Digital wellbeing is learning how we can use technology in a positive way and avoid it impacting on our physical and mental health.

Digital Wellbeing Top Tips

1. [Create screen free zones](#). It's important to keep phones and tablets in public spaces so you can keep an eye on what your child is doing online.



2. [Create screen free times of the day](#). It is important to turn off all devices an hour before bed. The blue light that comes from devices can stop you getting a good night's sleep, it confuses the body into thinking it's daytime when it should be winding down for the night. Remove devices from bedrooms.

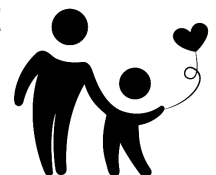
3. [Use Parental Controls](#). You can use parental controls to check the privacy settings of a device. You can set screen time limits. You can also make it so children only play appropriate games or apps. You can stop children from downloading inappropriate content and buying things.



4. [Make clear family rules](#). Talk together about what children are allowed to use online and when they are allowed to use it.

5. [Talk about being a good digital citizen](#). Talk to your children about what to do if something goes wrong. Encourage them to talk to a grown up. Discuss how to be responsible and polite online. They should act online as they would in real life. And treat others the way they would like to be treated.

6. [Watch and play together](#). Take time to sit with your children and play games together, watch things together, talk about what they like to do online and why they like to do it. The best tools for keeping children safe online are their parents.



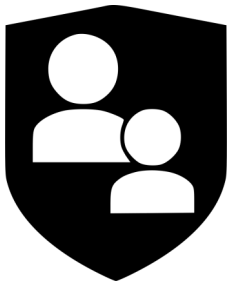
7. [Only allow age appropriate media](#). Check that all games, apps, YouTubers, films and TV shows are appropriate for your child. You can play or watch these yourself first, look for a PEGI rating or use www.common sense media.org/ to find out.

Privacy Settings and Parental controls

What are Privacy Settings?

Privacy settings help protect your identity and information. They can help keep your data safe and stop people being able to find where you are.

What are Parental Controls?



Parental controls is the name for a group of settings that put you in control of what your child can see. When used with privacy settings these can help you protect your children from the things they shouldn't see or experience online.

How do I use them?

There are lots of different places you can find these controls.

1. The first place to look is your internet provider - BT, Virgin, EE etc.

They all provide different privacy settings and parental controls. It is the first level of protection.

To find step by step instructions look here:

<https://www.internetmatters.org/parental-controls/broadband-mobile/>



2. You should then look at your device, computer, phone, tablet or console.

This will provide the next level of protection. They will often allow you to block children from downloading apps and buying things. They might also allow you to control screen time.

To find step by step instructions look here:

<https://www.internetmatters.org/parental-controls/smartphones-and-other-devices/>



3. Next, you should look at search engines (e.g. Google, YouTube). You can use these to filter out inappropriate content using Safe Search.



To find step by step instructions look here:

<https://www.internetmatters.org/parental-controls/entertainment-search-engines/>

4. You can also set privacy settings and parental controls on online platforms (Amazon Prime, Netflix, BBC iPlayer, NowTV etc). You can stop children watching inappropriate things as well as stop them from buying content.



To find step by step instructions look here:

<https://www.internetmatters.org/parental-controls/entertainment-search-engines/>

5. If you or your child has a social media account (Facebook, Instagram, Snapchat, WhatsApp, TikTok, etc) it's really important to check your settings. Make sure your accounts are private, and that you don't give away personal information.



To find step by step instructions look here:

<https://www.internetmatters.org/parental-controls/social-media/>



Remember:

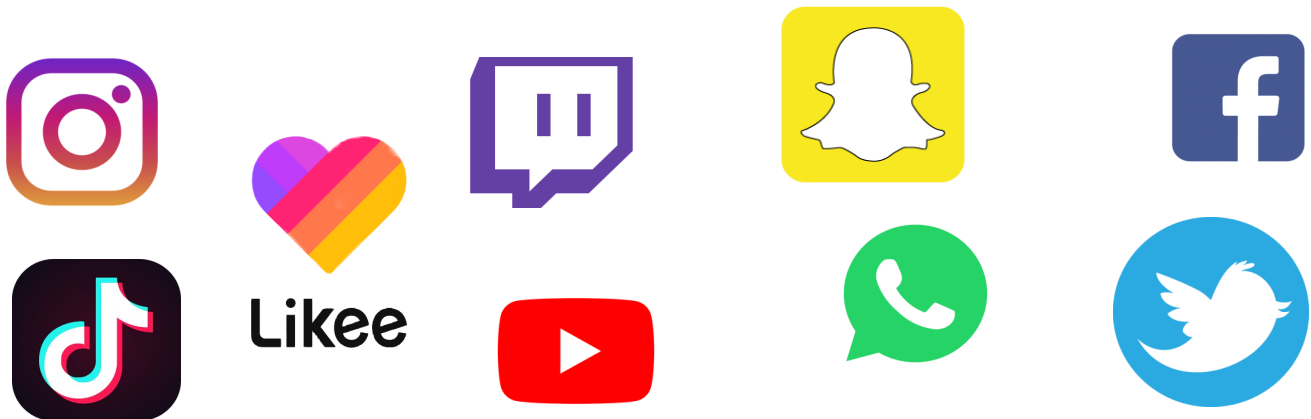
**The internet is always developing and changing,
to ensure your children are as safe as possible
you will need to regularly check all
Privacy Controls and Parental Settings.**

Social Media and Sharing Information

It is important to know that all Social Media sites require children to be at least 13 years old before they join. Some sites have older age requirements (Whatsapp has a requirement of 16 years old.)

Social Media sites allow people to share photos, videos, personal information and communicate with others. They include sites such as:

- Instagram
- Facebook
- Snapchat
- YouTube
- Whatsapp
- TikTok
- Twitter
- Twitch
- Likee



Please talk to your child about any social media accounts they may have. They may have set them up without your help.

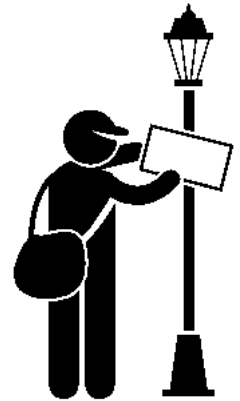
It is important to regularly check the privacy settings of both your own account and any accounts your children may have. Ensure that they are set to private and only allow sharing with friends, you will need to check that the location settings are private too. These settings regularly change and so need constant checking.

Most social media accounts are set to **PUBLIC** as default, which means you have to change the settings to **PRIVATE** as soon as the account is set up.

Sharing Information

Do you or your child share photos online? What kinds of photos are they? Where are they being shared?

We use the 'Lamppost test' - would you be happy for this picture to be posted on every lamppost in your town? If not, DON'T share it!



It is important to talk about the types of information both you and your children are sharing. Remember, everything posted online could stay online forever, it can be copied and become public and shared around the world. It's important to remember, that as parents you need to be mindful of photos you are posting of your children online because these pictures could cause embarrassment as they get older.

Never share PRIVATE information online

This includes:

- **Your full name**
- **Date of birth**
- **Address**
- **Where your child goes to school**
(including photos of children in school uniform)



As a parent you are the most effective tool to help protect your child online. You need to continually talk to your child about what they like to do online, who they are talking to and what they are sharing.

PEGI Ratings

What are they and where can we find them?

Whenever you buy games you will see a PEGI rating.

These give you:

1. A suggested age and a description of the content within the game. These appear on all games and apps. They appear when you buy a game online, in a shop or directly from a console.
2. Warnings about the type of content you will find within a game or app.

Below shows what the ratings might look like.



It's really important to check what games your children are playing and whether or not they are appropriate for their age.

What do the age ratings mean?

PEGI 3



Games given this rating are considered suitable for all age groups. They may contain some violence in a comical context or child-friendly setting. There may be nudity if shown in a completely natural and non-sexual manner, such as breastfeeding.

PEGI 7



Games may contain some possibly frightening scenes or sounds. Games can show violence as long as it's unrealistic and directed towards fantasy characters. There may be some non-realistic violence towards people or violent actions (eg: bombing of cities or non-human targets.)

PEGI 12



You could see more graphic and realistic looking violence towards fantasy characters. Violence towards humans mustn't look real unless it's showing trivial injury. Horror, including dread, strong threat and graphic injuries, is allowed.

Sexual innuendo, sexual posturing, references to gambling and some bad language can also be shown, although the latter must be mild.

PEGI 16



The game can feature death and injury to humans, including gory and bloody violence if the game is 'arcade style' (ie: not too realistic.) Smoking, drinking alcohol, the use of illegal drugs, glamorised representation of crime and strong bad language can be shown. It can contain erotic nudity and sexual activity, excluding the showing of genitals.

PEGI 18



These games can show 'gross' violence. This includes graphic methods of death or severe injury, including torture, decapitation and dismemberment, violence against vulnerable characters (including children), sexual violence and threat.

It may also include 'criminal techniques', glamorise illegal drug taking and show sexual activity featuring visible genitals.



November 2019