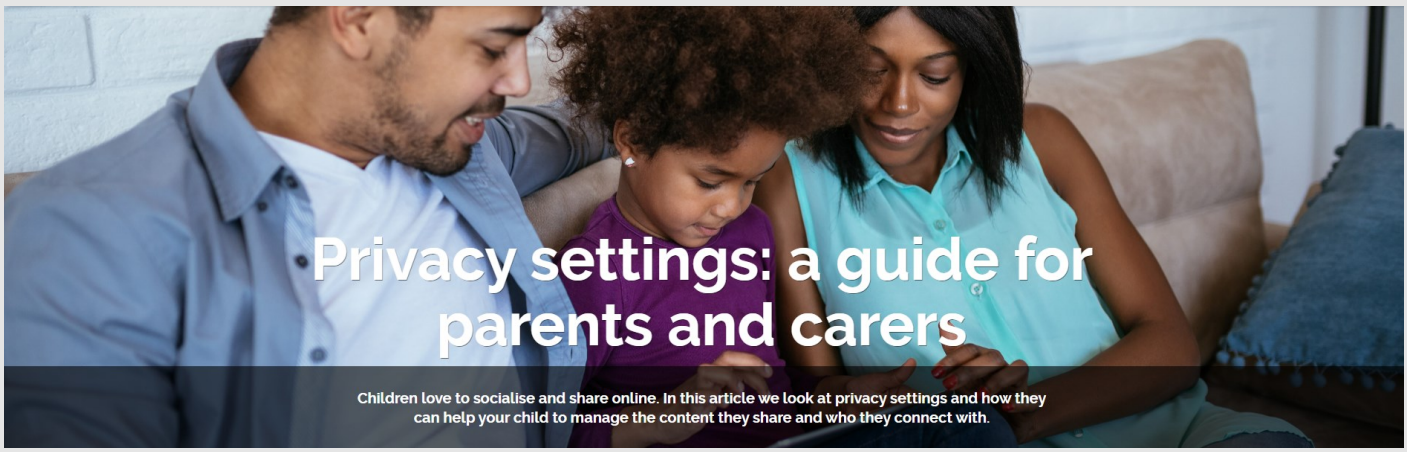
NORTHAMPTON SCHOOL FOR GIRLS

Respect for Self | Respect for Others | Respect for Learning

# Online Safety News Dec 2021

Many of us rely on technology over the winter break, for entertainment and keeping in touch with friends and family. In addition, quite a few students will receive items of technology as gifts at Christmas. As such, it's probably a good time to consider some of the points below from the online safety organisation, Thinkuknow.




The internet can be a great way for adults and children to connect with friends, family and new people. An increasing amount of children and young people are using social media, gaming and live streaming apps to chat and share content with others. But connecting and sharing with people online can come with risks too.

Once shared, personal information like their name, address, photos, or bank details online, could be used by others. For example, it could lead to the child beingbullied, groomed or blackmailed. It might also be used by cyber criminals.

**Privacy settings** can help you and your child to manage how much and what kind of information is shared, whilst enjoying their favourite sites, games and apps.

## What are privacy settings?

Privacy settings are controls available on many websites and apps to limit who can access your profile and what information visitors can see.

When online profiles are created, it's often assumed that they will be private by default. Unfortunately this isn't always the case – many are public until the settings are changed.

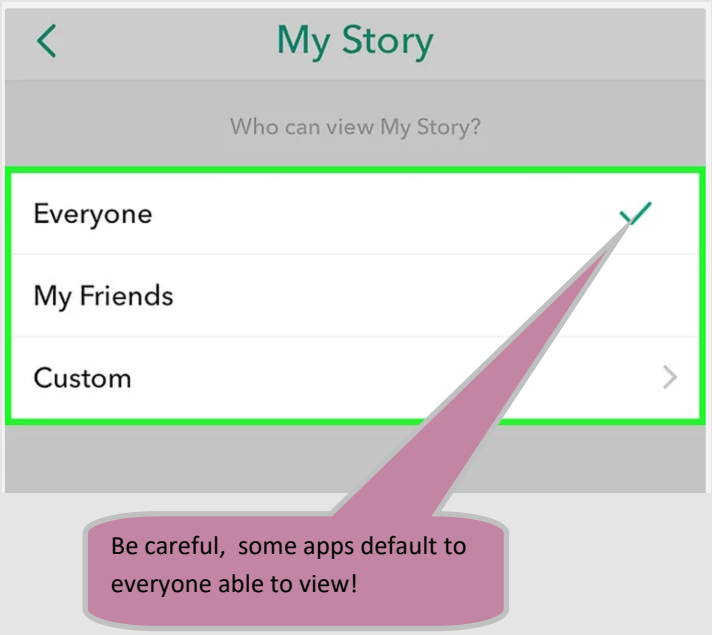
## How should I use privacy settings?

Follow these tips to help your child explore the internet safely. If you have an older child who creates their own accounts, use this information to talk to them about how they can use privacy settings.

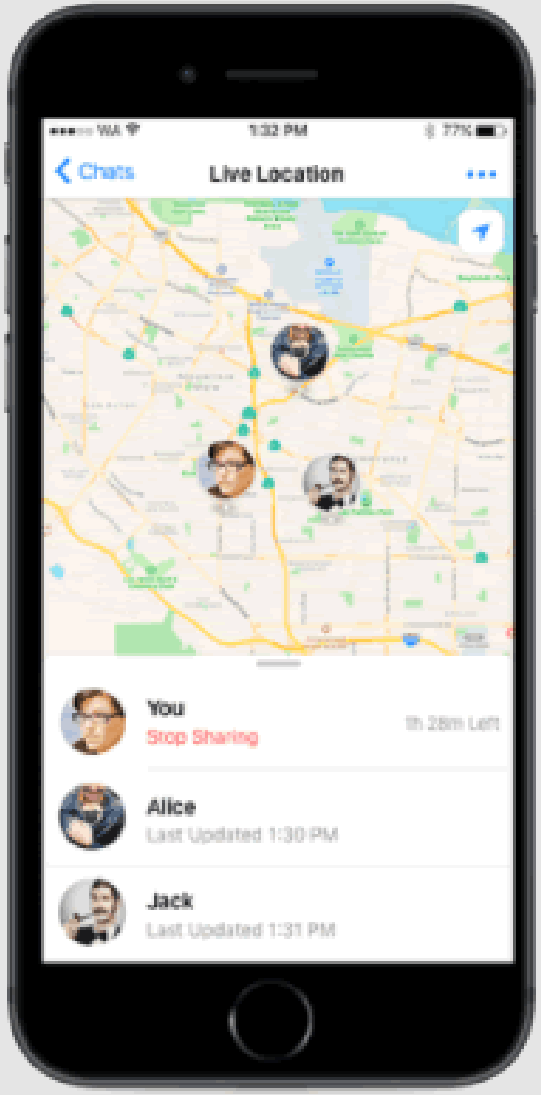
## 1. Check the audience.

Before your child shares content online, check who will be able to see what they post. You'll want to make sure that personal information can only be seen by small groups of friends who they know and trust.

Most apps allow you to change who can see your posts, who can contact you and who can look you up. You can even control who can see different parts of the content you share. For example, apps like Snapchat, Instagram and Facebook allow you to share 'stories' with smaller audiences, rather than your entire friends list.




## 2. Switch off location sharing.



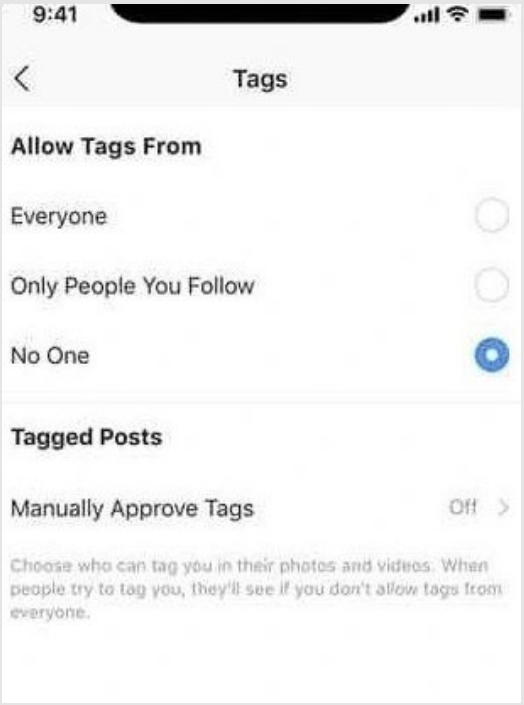

It's become increasingly common for apps to allow users to share their location. Many social media and live streaming platforms make it easy for you to broadcast what you're up to and where you are.

Some apps like Facebook and Instagram allow you to tag your photos with the place they were taken. These tags can list the exact address of your location, not just the city or general area they were taken in.

Other apps track users' locations and update them automatically. For example, Snapchat's 'Snap Map' location sharing feature can update your location whenever you have the app open. Its default setting is 'Ghost Mode' which prevents friends from seeing your location. However, some young people turn it on to let their friends see their whereabouts.

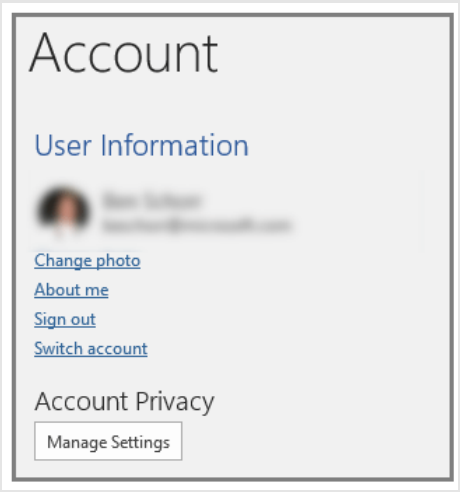
Remind your child that sharing their location online is risky. It could put them at risk of unwanted contact from strangers. Find out how to turn your child's location sharing services off, or make sure that they're only sharing it with people they know and trust.

## 3. Check the tagging settings.




It can be difficult to control information that others post about you online. Unless the content is abusive and violates community guidelines, it won't be taken down by the platform. However, privacy settings can be used to prevent private photos or information about your child from appearing on their profile.

Social media platforms like Facebook and Instagram have settings which allow you to review photos and information you're tagged in before it's posted to your profile.





## 4. Review all privacy settings regularly.

Many websites and apps periodically make changes to the privacy and security settings that they offer. Frequently review your child's privacy settings to ensure they're unlikely to encounter the risks associated with sharing personal information widely.

Some sites or apps like Facebook allow you to view how your profile looks to the public (people you're not friends with). Use this tool to check that you and your child are happy with the information they share to people they don't know.

Adults should regularly review their privacy settings too. If you posting pictures of your child, you may wish to think about how this could affect their online footprint for years to come. Further advice can be found in our 'Sharing pictures of your child online' article.

Even when privacy settings are put in place, it is important to remember that information posted online is never completely private. Further information on talking to your child about sharing personal information online can be found in our personal information article.

For specific advice about privacy settings on each of the popular apps, read these guides from Internet Matters.


## 3 ways to make gaming safer for your child

**1. Talk with your child about gaming.** Talk with your child to learn the games they like and the content and features of these. This will help you to understand more about how your child plays games and how appropriate different games are. You can use NSPCC's online safety hub to find out more information on safer gaming.

**2. Learn together.** Use our resources to teach your child about safer gaming at all ages. For primary age children you can use our Jessie & Friends (ages 4-7) and Play, Like, Share (ages 8-10) resources. Secondary age children can access advice about gaming through our website.

**3. Set boundaries and safety settings.** Internet Matters provides step-by-step guides for putting safety settings in place for each console or device. Spend time setting these up with your child and make sure they know how to block and report on the games they are playing. You should also talk with your child to create an agreement for gaming; think about how much time they can spend, which games they can access, if you will allow in-app purchases and what spaces they can play in. For primary aged children it is advisable to have them play in shared spaces or in the same room as you.

## How risky is in-game chat?

Gaming is often a social activity for children and talking with friends is part of their enjoyment. However, in-game chat can pose risks such as:

- chatting with people they don't know. This can include adults that are seeking to make contact with children with the intention of sexual grooming.
- inappropriate or unmoderated chat. Whilst a lot of chat is moderated, chat is live and there is a risk of exposure to sexual language, swearing or bullying.
- requests to make chat private. Once chat is moved off a monitored platform, no one is moderating it. This can be used to pressurise children into sharing personal information, photos, video or chat that they don't want to.
- offering gifts or trades. This may be used by offenders to build trust and a relationship with a child, as part of grooming.

Learn more about in-game chat and what you can do to make it safer by reading our parents and carers guide to in-game chat.

## How do I know what games are age appropriate for my child?

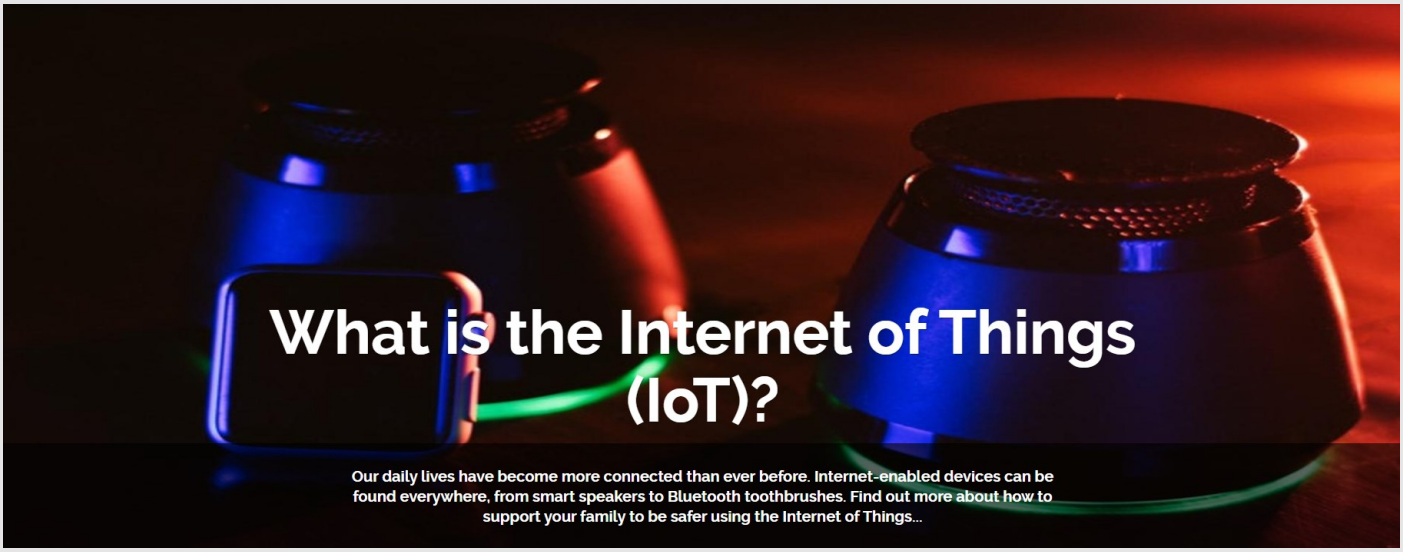
Our article on what's appropriate for your child will help you to understand more about the Pan European Game Information (PEGI) age rating system, which helps parents and carers to make informed decisions around games, giving age ratings and content descriptors.

Consider your child's individual needs, emotional maturity and experiences to support the decisions you make around gaming. For example, a game may be rated age appropriate but have content that you know your child will find frightening or won't understand.


## Should I be worried about gifts and trades in gaming?

Items such as game currency, skins, loot boxes, tools and weapons are often used in games to help a player progress through the game or give increased status amongst other gamers. Often these require in-app purchases, which many children won't have access to, or require your permission for, so accepting trades or gifts may be tempting.

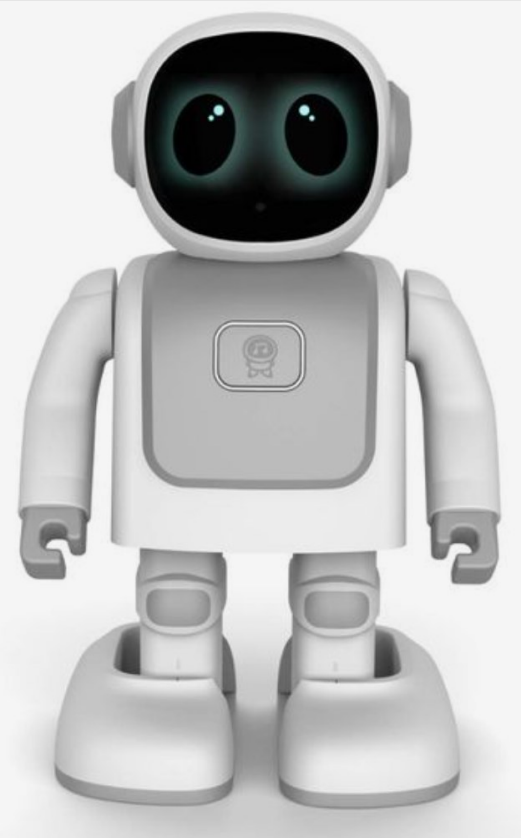
Whilst not always the case, trades or gifts within gaming can be used by child sex offenders to gain contact with a child. They may offer gifts asking nothing in return, this can be part of the grooming process and can help to build a close relationship with a young person. They may also try to use gifts as a way to persuade a child to do something such as going on a webcam, taking photos or videos of themselves, moving conversation to a different online platform or to an offline platform such as messaging over phone.




## What is the Internet of Things?


The Internet of Things, often referred to as IoT, are everyday objects that connect to the internet. These connected devices can be activated using voice commands, or controlled by downloading and using an app or via a Bluetooth or Wi-Fi connection. Examples of the Internet of Things include:

- Smart speakers,
- Smart meters (for home electricity and heating),
- and wearables such as smart watches or fitness trackers.



## What is the Internet of Toys?

The Internet of Toys are toys that connect to the internet. Similar to the Internet of Things, these toys can be controlled using a smartphone app, voice commands or using a Bluetooth connection.

Connected toys are different from other toys because they collect, use, and share data via the internet. This data might range from personal details like user age or location, to microphones and cameras recording what users see and hear.

Examples of the Internet of Toys include:

- Connected action figures and dolls,
- Bluetooth-enabled toys or tablets;
- Robotic toys such as drones,
- and learning development toys that aim to educate children.

## What are the risks associated with the Internet of Things?

Although connected devices and toys provide children with opportunities for learning and interactive play, there are some associated risks.

• Concerns have been raised about whether these devices are collecting **too much personal information** from children.
• Some children (either accidentally or on purpose) are able to search for and access **age-inappropriate material** via a connected device such as a smart speaker.
• Children may make **'in-app purchases'** and spend money, which is often taken from their parents' bank account without their knowledge or consent.
• Some of these devices may be more vulnerable to hacking and monitoring, as there are currently no security standards in place for connected devices.
Luckily, there are things you can do to minimise these risks.

## How can I make my connected home more secure?

**There are things you can do to help make your connected home safer for your child:**

**1. Do your research:** Research different products online and read reviews. This is a great way to find out more about a product including age restrictions and credibility, as well as hearing directly from other parents. Product manuals will also give you information about the privacy of the device and its use.

**2. Set up parental controls:** Make use of the parental controls available on your home broadband and any internet enabled device in your home. Enable the 'SafeSearch' function on your connected device and search engines to limit the material your child can access online.

**3. Update your privacy settings:** When you buy a connected device or toy, change the default password. Use a strong password that cannot easily be guessed and do not share this with others. Set your Bluetooth-enabled devices to 'undiscoverable' so your child doesn't share data or pair with an unknown device.

**4. Review and/or delete the data saved on devices:** Some connected devices or toys work by listening to your child's voice commands, so these devices usually record and keep these audio files to work properly. Refer to the manual and find out how to review and/or delete audio files. If there's a microphone on your child's connected device, you can turn on the 'mute' button. This will stop the device from recording and storing audio files.

**5. Talk to your child:** Include connected devices in your online safety conversations, reinforcing the message that if your child sees or hears anything that makes them feel worried, they can speak to you or another adult they trust. Read further information on starting the conversation about online safety.

For guidance on setting up parental controls or reviewing the privacy settings of a connected device or toy, you can find further information on the NSPCC's online safety hub.

For further advice on any of the topics discussed in this newsletter, or any other online safety issues, please refer to the online safety page on our school website.

Link here

The page links to a number of different organisations that can provide advice on keeping your children safe online and reporting issues.

Wishing you all a happy and peaceful Christmas.

Kind regards

Bruce Wainwright

Online safety coordinator

Head of Computing and ICT coordinator