Clarity Independent School

14th February 2024

E-safety Newsletter Spring term 2024

Dear Parents and Carers,

We have a lot of information to share with you this term. There's a lot to digest but please do read through all the advice and discuss it with your children to support them to think critically about what they're doing online and to help them to talk about their internet experiences openly with you.

It was the national 'Safer Internet Day' on 6th February 2024. Just like most schools across the UK, throughout this week, students have been exploring what 'safe internet use' really looks like for them and their peers. To explore this further with your child, and to encourage siblings and other family members to think about their internet safety, the website below has some great advice and resources:

https://saferinternet.org.uk/safer-internet-day/safer-internet-day-2024

The students have also been finding out more about the Online Safety Act 2023 and what this means. It's important that we are aware of this so that we can support the children to understand what it means.

The Online Safety Act 2023:

In October 2023, the Online Safety Bill was made law and became the Online Safety Act 2023.

Its goal is to make the internet safer for children by making tech firms take more responsibility for the content on their platforms. Social media platforms will now have to:

- Remove illegal content quickly or prevent it from appearing in the first place
- Prevent children from accessing harmful and age-inappropriate content
- Enforce age limits and use age-checking measures
- Be more transparent about the potential risks and dangers associated with the platforms
- Give parents/carers and children clear and accessible ways to report any problems

A number of new offences have been introduced by the Act:

These are:

- Cyber-flashing, which is when someone intentionally sends an unsolicited image or video to someone else via social media, dating apps, or a data sharing service like Airdrop. It's classed as an offence if the person who sends the image or video intends the recipient to be alarmed, distressed or humiliated, or it's sent for their own gratification
- Sharing "deepfake" pornography that's been created by AI without someone's permission

- Sending a message with information that the person knows to be false, to cause psychological or physical harm
- Sending a death threat or threat of serious harm
- Assisting or encouraging someone else to self-harm
- Sending a flashing image to try to trigger a seizure in someone with epilepsy (sometimes known as “epilepsy trolling”)

Attached to this newsletter, you will find two parent factsheets:

1. The first factsheet will give you more information about Cyber-flashing offenses (something which The 2 Johns warned us about in their E-safety workshops last term as this is sadly becoming so common an experience that our young people are frequently subjected to that it is becoming normalized and almost expected by our children).
2. The second factsheet provides information and advice about the app “Monkey”, which sounds like it is aimed at young children but though it states it’s for aged 17+ and it poses some worrying risks.

As always, if you have any concerns that you would like to receive advice for, please do not hesitate to get in touch.

I hope that you and your children have a lovely half term break.

Yours sincerely

Sharyn Ailara, Deputy Head Teacher
BSc (Hons), PGCE, SENDCo Accreditation

PARENT FACTSHEET

Keep your child safe from cyber-flashing

What is it?

Cyber-flashing happens when a stranger sends an explicit picture, uninvited, to a device (such as a phone or tablet) via Wi-Fi or Bluetooth. It's sexual harassment.

It's most likely to happen on public transport or in crowded places.

The file-sharing app AirDrop for iPhone and iPads is most commonly associated with cyber-flashing, but there are lots of different file-sharing apps out there.

With AirDrop, it can be easy for anyone to send unsolicited images. The automatic preview feature means you also see images without actually opening them.

The **Online Safety Act 2023** will make cyber-flashing a new criminal offence. It will be illegal for anyone to send or show a photo or film of any person's genitals to cause alarm, distress or humiliation, or for the purpose of their own sexual gratification. This offence will come into force once secondary legislation has been written.

3 steps to keep your child safe

1. Restrict who can send files to your child's phone

Most file-sharing apps allow users to restrict who can send files to them by Wi-Fi or Bluetooth. Find out which apps your child uses, then make sure your child knows how to use these settings.

For AirDrop on **iPhones**:

- Open '**Control Centre**' (swipe down from the upper-right corner or up from the bottom of the screen, depending on the model)
- Press firmly on the **network settings card** (this is in the shape of a square) in the upper-left corner. This will open more connectivity controls
- Tap and hold the **AirDrop** icon
- Select '**Contacts Only**', or '**Receiving Off**' (to not receive AirDrop requests)

Or, do this by going to Settings > General > AirDrop

Some of the other most popular file-transfer apps include:

- Google Drive
- Dropbox
- Microsoft OneDrive
- AirDroid
- Zapya

Make sure your child knows to only accept files from people they know.

2. Turn off Bluetooth when not using it

Otherwise, it can be easy for strangers nearby to send images to your child's phone.

To do this on **iPhone**, open 'Control Centre' (see above), then tap the Bluetooth icon (it looks like a 'B'). The icon dims when it's off.

On **Android**, swipe down from the top (you might need to do this twice or scroll across). Then tap the Bluetooth 'B' icon to turn it off. It'll be grey when Bluetooth is off.

3. Make sure your child knows what to do if it happens to them

If your child doesn't feel in immediate danger, they should take a screenshot and report the incident to the police using the non-emergency numbers:

- If it happens on public transport, text 61016 or call 0800 40 50 40
- If it happens anywhere else, call 101

If your child feels scared or in immediate danger, they should call 999. They should also move to a safe place – and find someone in authority to talk to, such as platform staff, a security guard or a shop manager.

If it happens in school, your child should talk to a trusted adult immediately. If it has happened outside of school, you or your child can still ask the school for support.

It can be difficult for children to tell someone about sexual harassment

If your child tells you about being a victim of an incident of cyber-flashing, make sure you:

- Listen to them carefully
- Reassure them you'll support them
- Remain non-judgmental

Sources

This factsheet was produced by The Key Safeguarding: **http://thekeysupport.com/safeguarding**

- Keeping Children Safe in Education, GOV.UK – DfE
  https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
- Online Safety Act 2023, GOV.UK – UK Parliament
  https://www.legislation.gov.uk/ukpga/2023/50/enacted
- How to use AirDrop on your iPhone, iPad, or iPod touch, Apple
  https://support.apple.com/en-gb/HT204144#setoptions
- Use Bluetooth and Wi-Fi in Control Centre, Apple
  https://support.apple.com/en-us/HT208086
- Connect through Bluetooth on your Android device, Android Help
  https://support.google.com/android/answer/9075925?hl=en-GB
- 61016 text service, British Transport Police
  https://www.btp.police.uk/police-forces/british-transport-police/areas/campaigns/61016-text-service/

At National Online Safety, we believe in empowering parents, carers and trusted adults with the information to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one of many apps which we believe trusted adults should be aware of. Please visit nationalcollege.com for further guides, hints and tips for adults.

What Parents & Carers Need to Know about MONKEY

Also known as Monkey Cool, this platform aims to fill the gap left by Omegle (which has now shut down) by placing users in random video chats with strangers. Participants use their mobile number and Snapchat username to connect to the service, where they can make matches, message other people and join group chats. The mobile version has been removed from the App Store due to safety concerns, but iPhone owners can still access the site via their web browser. The app remains available on Google Play, where its listing claims that Monkey has more than 30 million users worldwide.

AGE RESTRICTION 17+

(although the lack of age verification means that someone younger could easily log in with a fake date of birth)

WHAT ARE THE RISKS?

AGE-INAPPROPRIATE CONTENT

The app claims to use AI to detect sexual content or activity that violates its policies, along with having a 24/7 moderation team. However, reports in the media continue to indicate that explicit content remains commonplace on Monkey (including sexually graphic or violent material) and is therefore accessible to anybody who uses the app – including those aged under 18.

IN-APP SPENDING

While Monkey is free to download, it nevertheless offers in-app purchases promising to unlock access to premium features. For example, users who wish to make use of 'Knock Knock chat' (Monkey's text-based messaging option), rather than the app's Chatroulette-style random video calling feature, will need to pay to be able to do so.

CONTACT WITH STRANGERS

The obvious risk in accepting random video chat partners is that users cannot know what or who they will see on their next connection. Talking to strangers is, of course, potentially dangerous – especially for children who might be persuaded to meet up with these people offline. The app lets users find each other by location, increasing the chances of a child being matched with a stranger from their local area.

INTRUSIONS ON PRIVACY

According to Monkey's privacy policy, personal information (such as name, profile picture and date of birth), user-contributed content (any photos, texts, videos and screenshots shared) and each user's browser and IP address are collected. That is a considerable amount of data for Monkey to gather on its users – and all of this information is shared with third parties.

Advice for Parents & Carers

DISCUSS THE DANGERS

Even if you're comfortable with your child using Monkey, it's still important to talk about the potential dangers. It's crucial, for instance, that young people recognise the risks that stem from video chatting with strangers; that they understand not to share identifying information (like their street or school name); and that they know what to do if they are exposed to inappropriate content.

RESTRICT IN-APP PURCHASING

If your child is accessing Monkey via an Android device, you can prevent them from making in-app purchases through the device's settings. If you *do* allow your child to use the site, we'd recommend that you enable this feature: young people have been known to spend significant amounts of money in their desire to unlock more features in apps such as this.

REPORT INAPPROPRIATE CONTENT

Monkey states in the safety section of its site that "people are given the power" and that, to a large extent, Monkey is "self-governing." If a user is exposed to sexually explicit or inappropriate content on the platform, they can select the 'police' emoji in the top right corner of their screen to submit a report for Monkey's moderation team to review.

SPOT THE SIGNS

If you're concerned that your child is spending too much time on Monkey – or that they may have been exposed to inappropriate or distressing content – it's important to watch for potential indications that they've been affected emotionally. They could be unusually irritable or unable to concentrate, for example, or failing to complete their homework or even to eat regular meals.

Meet Our Expert

Dr Claire Sutherland is an online safety consultant, educator and researcher who has developed and implemented anti-bullying and cyber safety policies for schools. She has written various academic papers and carried out research for the Australian government comparing internet use and sexting behaviour of young people in the UK, USA and Australia.

The National College

NOS National Online Safety

#WakeUpWednesday

@natonlinesafety /NationalOnlineSafety @nationalonlinesafety @national_online_safety