St Mary Redcliffe and Temple School

Welcome to this week's SMRT safeguarding update…

WAKE UP WEDNESDAY

Online Safety and Apps

At SMRT we train all staff regularly about online safety, have VIP lessons in place for every year group about how to stay safe online and have a range of assemblies, events and tutorials in place to help students understand and avoid risks online. For parents and carers, setting clear boundaries, and monitoring online activity is essential. This includes discussing the dangers of sharing personal information, cyberbullying, and online grooming, as well as teaching young people how to identify and report inappropriate content.

Important reminder for all parents and carers: Apps and on-line Safety:

While our safeguarding updates cover a range of online safety concerns and government guidance, please could I draw your attention to these sites in particular: Discord, Omegle, OwnTV, Thundr, Reality and monkey. All of these sites have an on-line gaming focus and use live streamers. These are specifically for over 18 users and are known to be places where older males have groomed and abused young people in the past.

In order to place further controls on your child's phone or device, please follow the attached instructions for Android and iphone users.

We would encourage you to check what platforms and sites your young people have been using and report any concerns to CEOP (Child Exploitation and Online Protection Command).

https://www.ceop.police.uk/ceop-reporting/

Top Tips include:

1. Open Communication and Education:

- **Talk to your children about online safety:** Regularly discuss the potential risks of the internet, including cyberbullying, inappropriate content, and online predators.
- **Encourage open communication:** Make sure your children feel comfortable talking to you about anything that worries or upsets them online.
- **Teach them about online reputation:** Explain how online actions can impact their reputation and future.
- **Explain the importance of strong passwords and privacy settings:** Emphasize that passwords are like digital keys and should be kept private.

2. Setting Boundaries and Monitoring:

- **Establish clear rules:**

Agree on age-appropriate boundaries for online activities, including time limits and websites/apps that are allowed.

- **Supervise online activity:**

Keep computers and devices in a common area of the house, and monitor their use, especially for younger children.

- **Utilise parental controls:**

Explore and implement parental control features on devices, browsers, and streaming services.

In particular, see the ways you can limit access to unsafe apps and have controls over these on their phones (see attached guides).

- **Be aware of your child's online friends:**

Know who they are interacting with online, and if they plan to meet someone in person, always meet in a public place with other adults present.

3. Staying Informed and Taking Action:

- **Familiarize yourself with online safety tools and resources:**

Explore websites like Internet Matters, Childnet, and NSPCC, which offer guidance and support.

- **Report any concerns:**

If you encounter inappropriate content or suspect online grooming, report it to the appropriate authorities, such as the police or the National Crime Agency (NCA)-CEOP.

- **Stay informed about new trends and apps:**

Keep up-to-date on the latest online platforms and potential dangers they may pose.

4. Promoting Digital Wellbeing:

- **Encourage a healthy balance of online and offline activities:** Help your children understand the importance of spending time on other activities and hobbies.
- **Teach digital kindness and respect:** Encourage empathy and positive online interactions.
- **Promote responsible online behaviour:** Make sure your children understand that what they do online can have real-world consequences.

By taking these steps, we can work together to help create a safer online environment for children and empower them to navigate the digital world with confidence and responsibility.

As always, if you have any immediate concerns about safeguarding issues, students, or the school site, please get in touch via:

safeguarding@smrt.bristol.sch.uk

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 www.nationalonlinesafety.com for further guides, hints and tips for adults.

What Parents & Carers Need to Know about DISCORD

AGE RATING 13+

Servers and channels marked as 'NSFW' require users to be 18 or older to join.

Discord is a free app which allows users to communicate in real time via text, video or voice chat. Available on desktop and mobile devices, it was originally designed to help gamers cooperate – but has evolved into a more general networking platform for a range of online communities, discussing topics like TV series, music, Web3 and more. Discord is organised around closed groups, referred to as 'servers'. To join a server, users must be invited or provided with a unique link. It's a space for users to interact with friends, meet others with shared interests and collaborate privately online – but it's also a place where young people can be exposed to risks if the right precautions aren't taken.

WHAT ARE THE RISKS?

CYBERBULLYING

Discord's easy accessibility and connectivity, unfortunately, makes it an ideal place for cyberbullying to occur – especially as audio and video streams disappear once they've ended, meaning that bullying could take place without leaving any evidence. Closed groups can also be created, giving young people the opportunity to exclude their peers or send cruel messages without adult oversight.

DIFFICULT TO MODERATE

Like many private communication apps, Discord's real-time messaging can be difficult to control. The system enables content moderation through each individual server – so different groups can set their own rules for what's acceptable, and some groups may not monitor for unsuitable content. Anything that happens in an audio or video stream is also virtually untraceable once the stream has concluded.

INAPPROPRIATE CONTENT

Discord mainly hosts private groups, making it easier for unsuitable or explicit content to be shared on channels. Pornography, racism and inappropriate language can be found in some groups. Server owners are required to add an age-restriction gate to channels where 18+ content is being shared – but this solution isn't foolproof, as the platform doesn't always verify users' ages when they sign up.

ACCESSIBLE TO PREDATORS

On many chat platforms, users can lie about their age or true identity – and Discord is no exception. Predators have attempted to abuse the platform by using it to contact and communicate with underage users – by initially chatting with a child on an age-appropriate channel, for example. While Discord has improved its safety settings, some users will still try to bypass them for malicious reasons.

CRIMINAL ACTIVITY

Discord does have strict Terms of Service and Community Guidelines to protect its users – but, sadly, not everyone adheres to them. Criminal activity including grooming, hate speech, harassment, exploitative content, doxxing and extremist or violent material have all been found on Discord servers over the last two years. In 2020, Discord received almost 27,000 reports of illegal activity on the platform.

Advice for Parents & Carers

REVIEW SAFETY SETTINGS

Discord has a series of safety settings, enabling users to choose who can direct message them or send them friend requests. Your child's experience on Discord will be much safer if the app's privacy and safety settings are configured to only allow messages or friend requests from server members. This will minimise the chances of potential predators from outside the group contacting them.

EXPLAIN AGE FILTERING

While Discord requires users to be at least 13 to sign up, many servers geared towards older users are flagged as NSFW (not safe for work), which indicates they probably contain material that's inappropriate for children. It can be easy to click through settings without properly reviewing them, so ensure your child understands why age filtering is important and that it's there to protect them.

SCREEN OUT EXPLICIT CONTENT

In the privacy and safety settings, Discord users are offered the ability to filter direct messages for inappropriate content: a setting that should be enabled if your child uses the platform. Discord automatically tries to flag images that are explicit, but the setting must be manually enabled for text. If a young user is sent explicit content in a direct message, Discord will scan and (if necessary) delete it.

MONITOR ONLINE ACTIVITY

It's wise to regularly review your child's activity on Discord. This can include checking their safety settings to ensure they're correctly enabled, talking about which servers they've joined and reviewing some of their friends and direct messages. Ask if anything has made them feel uncomfortable or unsafe. Things can change quickly online, so plan routine check-ins and follow up frequently.

DISCUSS GOOD ONLINE BEHAVIOUR

The anonymity offered by the internet often leads people to communicate more openly online and behave differently than they would at school or home. It's crucial to bear in mind, though, that every internet user is still a real person. Talk to your child about the severe and lasting consequences that cyberbullying or exchanging inappropriate material online can have in the real world.

HAVE CANDID CONVERSATIONS

It can sometimes be awkward to discuss topics like grooming, pornography, racism or explicit content with your child – but it's important to ensure they're aware of the harms these things can pose. Talking openly about these subjects is a great way to help your child feel more comfortable about coming to you if they experience an unwanted encounter on Discord (or anywhere else online).

Meet Our Expert

Carol Cripps is a Canadian-born, London-based tech journalist at gmw3.com: a website specialising in all things Web3, gaming and XR (extended reality). With a focus on brands and culture, she researches and writes about the ways that our current innovations – including the metaverse and Web3 – are impacting people, places and things.

National Online Safety®

#WakeUpWednesday

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 issue of many which we believe trusted adults should be aware of. Please visit www.nationalonlinesafety.com for further guides, hints and tips for adults.

How to Set up PARENTAL CONTROLS for APPS

iPhone

Apple devices come with built-in apps already available: Mail, FaceTime and Safari, for example. However, you can choose which apps and features appear on your child's device and which ones don't. You can also manipulate the features in Game Centre to enhance your child's safety and privacy when playing games, as well as blocking iTunes or App Store purchases if you wish.

How to Restrict Built-in Apps/Features

1. Open Settings
2. Tap Screen Time
3. Tap Content & Privacy Restrictions
4. Tap Allowed Apps (you may need to toggle this to 'on' at the top)
5. Enable or disable the apps you wish to appear (or disappear) on your child's device

How to Restrict Game Centre

1. Open Settings
2. Tap Screen Time
3. Tap Content & Privacy Restrictions
4. Tap Content Restrictions (you may need to switch the toggle at the top to the 'on' position)
5. Scroll down to Game Centre
6. Choose between Allow, Don't Allow, or Allow with Friends Only in the settings for each feature

How to Restrict iTunes & App Store Purchases

1. Open Settings
2. Tap Screen Time
3. Tap Content & Privacy Restrictions
4. Tap iTunes & App Store Purchases
5. Select Allow or Don't Allow for each feature (you can also lock these settings with a password)

National Online Safety
www.nationalonlinesafety.com

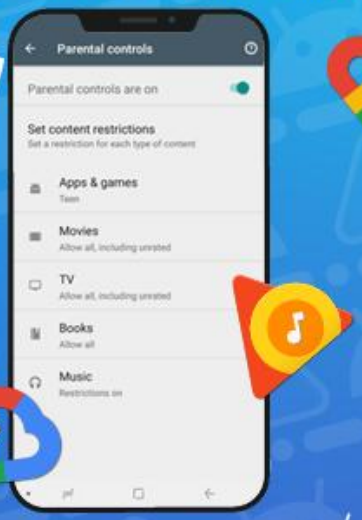
www.nationalonlinesafety.com @natonlinesafety /NationalOnlineSafety @nationalonlinesafety

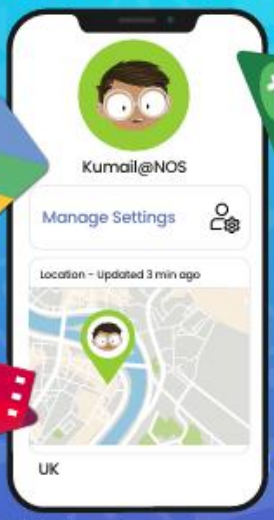
At National Online Safety, we believe in empowering parents, carers and trusted adults with the information to hold an informed conversation about online safety with their children, should they feel it is needed. This guide focuses on one issue of many which we believe trusted adults should be aware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

How to Set up PARENTAL CONTROLS for APPS

Android Phone

On Android phones, restricting access to particular apps usually requires going onto Google Play. From there, it's fairly easy to navigate your way through the settings to manage the parental controls and authentications relating to any apps on the device. These features can prevent your child from downloading or buying anything unsuitable for their age. Updated versions of apps or games that your child has already installed may occasionally contain something inappropriate, so we've explained how to stop those, too.





How to Block App Downloads (This Also Disables In-app Purchases):

1. Open Google Play Store
2. Tap the profile icon in the top right
3. Tap Settings
4. Scroll down to the Family section and tap Parental controls
5. Toggle 'Parental controls are off' to 'Parental controls are on'
6. Create a PIN and tap OK
7. Confirm your PIN and tap OK again
8. Tap Apps & Games
9. Set the age limit you wish to set
10. Tap Save to apply your changes

How to Stop Auto-updates

1. Open Google Play Store
2. Tap the profile icon in the top right
3. Tap Settings
4. Tap Auto-Update Apps
5. Select 'Don't auto-update apps' and then tap Done

Restricting Apps Through Google Family Link

1. Open Google Play Family Link for parents
2. Tap the three horizontal lines in the top left
3. Select your child's account
4. Tap Manage
5. Tap Controls on Google Play
6. Tap Apps & Games
7. Select the age limit you wish to set

National Online Safety
www.nationalonlinesafety.com

www.nationalonlinesafety.com @natonlinesafety /NationalOnlineSafety @nationalonlinesafety