SAFEGUARDING
SEPTEMBER 2021

Welcome to our Parent Safeguarding Newsletter - September 2021

SAFEGUARDING TEAM

Catmose Primary Designated Safeguarding Lead
Mrs Jackson - kjackson@catmoseprimary.com

Safeguarding Officers
Mrs Coyne - rcoyne@catmoseprimary.com
Mrs Derry - nderry@catmoseprimary.com

Catmose Primary School Office - 01572 772583

INSIDE THIS ISSUE

BACK TO SCHOOL

Online Safety Tips for Children

Wow, it's September already! The month when autumn officially starts and ... oh yeah, the beginning of a new school year. Every cloud has a silver lining though! Another term means new friends to make, different stuff to learn, fresh online trends to jump on and exciting new games to play on your phone, computer or console. We've compiled a list of our top tips to ensure that – whether you're going online to chat, research things or just have fun – you can do it safely.

Be cautious with your profile

Be careful not to give out too much info on your social media or gaming profiles. Details like your full name, address or school's name could all help strangers to actually find you offline. A trusted adult can help you make your profiles private – so only your family and actual friends can contact you.

Lock your devices

Taking your phone or tablet to school? Turn password protection on. It keeps your private info safe and stops anyone accessing your device without permission. Passwords should be memorable to you – but difficult for anyone else to guess. Get a trusted adult to write it down in case you forget it!

Be smart with screen time

Too much screen time, especially just before bed, can affect your quality of sleep. Losing sleep, or not sleeping well enough, messes with your concentration and energy levels. Try muting notifications so you don't get pinged late at night: you'll feel fresher and more focused the next day.

Know how to deal with bullies

Sadly there are people online who enjoy picking on other users. If you ever feel like you're being bullied online – by anyone, not just someone from school – talk to a trusted adult about it. Together, you can discuss possible steps, such as blocking or reporting the person who's targeting you.

Manage online relationships wisely

Most people in a relationship chat to their partner online. Just be mindful that once you send a pic or message (even if it's private), you no longer control who else might see it. Messaging someone you've never actually met – and who might not be who they say – is definitely best avoided.

React well to inappropriate content

When you're researching something online, there's always a chance of finding content that makes you feel uncomfortable or upset. If this happens, you can report it as inappropriate and (hopefully) get it taken down. Tell a trusted adult what happened: they'll help you decide what to do next.

Report offensive in-game chat

If you game online with your mates, you'll know things can get competitive and heated on the in-game chat. Playing against people you don't know (especially if they're older) raises the risk of offensive comments and even threats. Our advice? Find out how to block or mute those bad losers.

Learn to spot fake news

If you're looking into a topic for homework or a project, be careful not to get taken in by fake news: content that's deliberately created to mislead people. Check the story with credible sources, like the BBC or Sky News. Trust your instincts, too – if it seems too unbelievable to be true, it's probably fake.

Keep it 'real' with online friends

Everyone enjoys adding friends and followers on social media. It's important, though, that the people you interact with online really are your friends. If they're just random people you've connected with to increase your contacts, you don't know if they could be trolls or bullies (or worse).

National Online Safety®

#WakeUpWednesday

THINKUKNOW
ONLINE SAFETY ACTIVITIES PACKS

The ThinkUKNow home activity packs include simple 15 minute activities you can do with your child to support their online safety at home. Download your pack here.
https://www.thinkuknow.co.uk/parents/Support-tools/home-activity-worksheets/

These include fun activities, conversation starters and practical tips on topics such as:

Don't forget to use this as an opportunity to talk about permission, if using a photo of others, being kind and thinking about sharing with others.

- Sharing images
- Live streaming
- **Cyber security online safety** - we know that the coronavirus pandemic has increased the risks that children face online. One of the reasons for this is that number of moderators working to keep users safe was dramatically reduced during 'lockdown one'. The BBC published an article about the risks to children online in relation to self-harm. Young people are extremely vulnerable when using the Internet and social media unsupervised and content that is shared can have a significant impact on them. Read the full article here: https://www.bbc.co.uk/news/technology-55004693
- **The Charlie Waller Trust** have developed a resource to support parents and carers with the issue of self-harm. The guide can be found here: https://charliewaller.org/resources/coping-with-self-harm

- **Managing social media** - Over the past year, our lives have been disrupted greatly and usual routines have changed for most of us. Whilst social media can be an effective tool for staying connected to friends and family, it can also be a place where negative language and imagery is regularly shared which can have a negative impact on mental health and wellbeing. This booklet from Anna Freud aims to highlight some key social media issues and offers advice and guidance on how to minimise the impact of social media on mental health: https://www.annafreud.org/on-my-mind/managing-social-media/
- **Coping strategies** - Children and young people can find this time of the academic year overwhelming and it can be hard for them to know how to cope. But distracting yourself or doing something positive can really help. Childline have a space on their website full of lots of activities to do with children when they are feeling low or overwhelmed. To access these and the coping kit please click here: https://www.childline.org.uk/toolbox/coping-kit/

TALKING TO CHILDREN AND YOUNG PEOPLE ABOUT THEIR MENTAL HEALTH

Sometimes it can be difficult to know how to begin a conversation with your son or daughter about their mental health and emotional wellbeing. Here are some useful conversation starters from **Young Minds** that you could use.

Questions to ask your child

LOOKING FOR SUPPORT WITHOUT HAVING TO CALL?

YoungMinds new webchat service connects parents and carers with one of their advisors and helps you find the information you need to support your child's mental health.
Contact the YoungMinds Parents Helpline
www.youngminds.org.uk/webchat

YOUNGMiNDS
fighting for young people's mental health

WHERE CAN I SEEK SUPPORT FOR MY CHILD'S MENTAL HEALTH AND EMOTIONAL WELLBEING?

We know that recent months have been difficult for adults and children alike. Children have found the change to their daily routine, anxiety about the impact of coronavirus on their education and isolation from family and friends very challenging and in some cases they may need some additional support with their mental health and emotional wellbeing. In addition to your child's GP, there are a wide variety of support services and advice lines available for parents, carers and children to access. These services can vary according to where you live.

The College website's mental wellbeing page has information on local services available to support your child and top tips for good mental health:
https://www.catmosecollege.com/mental-well-being/

What Parents and Carers Need to Know About... ROCKET LEAGUE

Age Restriction PEGI 3

Rocket League is a free-to-play multiplayer vehicle football game. It was developed by Psyonix, now part of the Epic Games family (which also includes Fortnite and Gears of War). Rocket League is essentially a football game where, instead of running, the players drive rocket-powered cars. The game was a surprise hit that took the world by storm when it first released in 2015. Rocket League is available for the Xbox One, Xbox Series X, PlayStation 4 & PlayStation 5, Nintendo Switch, Windows PC, MacOS and Linux.

Fiercely Competitive Community

Competitive gaming isn't necessarily bad. However, playing purely to win (as opposed to simply having fun) can result in aggressive behaviour among some players if they're not successful in the game. Certain people can become hostile or "toxic" towards other players. Continually seeing this behaviour can cause children to think it is acceptable and lead to anger issues while playing.

Unsuitable Online Interactions

18+

A video game's age rating cannot take player-generated elements into account. Rocket League is rated PEGI 3, but its online features mean that appropriateness can't be guaranteed. Audio and text chat, player usernames, player-to-player trades and other user-created content may not be suitable for young players. The game *is* moderated, but catching everything can be difficult.

Grinding and Increased Screen-time

Features like the Rocket Pass and the ranking system can make Rocket League a grinding-focused game. This means players need to spend a lot of time on the game to progress through levels and collect rewards. Grinding encourages regular long gaming sessions for players seeking to climb the rankings (meaning increased screen time) but it doesn't always result in making much headway.

Scams and Bad Trades

Player-to-player trading is common in Rocket League. The game has lots of cosmetic items to collect, and some can be very valuable. Players can trade items among themselves, but younger gamers are not always the best judges of what constitutes a fair deal. This can lead to them being swindled in trades – or to children signing up to illegitimate trading websites, where they then get scammed.

In-App Purchasing

Free-to-play games (so called because they don't cost anything to download) like this depend on players making in-game purchases to turn a profit. Rocket League's in-game currency, called credits, are used to buy items in the game. Credits can be earned by playing the game or can be bought with real money – which could prove expensive if a child lets their love of the game and desire to progress get the better of them.

Advice For Parents & Carers

Use Parental Controls

Psyonix *has* added some safety measures into the game. The text and voice chat can be disabled, for example, limiting contact from strangers. However, it's not currently possible to block contact from other players about trades. It's a good idea, then, to talk with your child about the possibility of scams and bad trades either before they download the game or early in their Rocket League 'career'.

Stay Aware of Spending

Free-to-play games can become money sinks without children realising. For peace of mind, make sure you don't have any payment methods attached to your child's gaming account to avoid accidental purchases. Rocket League credits can be earned through gameplay or bought with real money: encourage your child to use their earned credits first before they ask you to top them up.

Monitor Gaming Time

It's impractical to sit and watch your child every time they play Rocket League. Keeping an eye on their gaming hours is crucial, however: it's easy to lose track of time while playing (even for adults), so "one more game" can soon turn into ten more games. Helping your child to balance their gaming time with their homework, chores and other activities is a life lesson in time management.

Encourage Regular Breaks

Sitting in the same position all day while gaming isn't healthy, but it is an easy habit to fall into. A short break every hour or half hour is important. It allows players to rest their eyes, brains, hands and arms. Learning the value of an occasional break from *any* activity is good practice for the future. Encouraging your child to rehydrate regularly can also help to lower any rising competitive tempers!

Meet Our Expert

Clare Godwin (a.k.a. Lunawolf) has worked as an editor and journalist in the gaming industry since 2015, providing websites with event coverage, reviews and gaming guides. She is the owner of Lunawolf Gaming and is currently working on various gaming-related projects including game development and writing non-fiction books. With experience in esports and content creation, Clare has seen the benefits *and* drawbacks of all aspects of gaming.

National Online Safety®

#WakeUpWednesday

SOURCES: https://support.rocketleague.com/hc/en-us/articles/360015613074, https://support.rocketleague.com/hc/en-us/articles/360053542814-Parental-Controls, https://support.rocketleague.com/hc/en-us/articles/360039907693-How-can-I-protect-my-child-from-online-interactions-, https://theglobalgaming.com/rocket-league/credit-system-free/

What Parents and Carers Need to Know about ...

SOCIAL MEDIA SCAMS

On any social media platform, you'll often come across links to genuine-looking websites. They might include an exclusive offer for one of your favourite shops or invite you to complete a quiz in return for a particular reward. In some cases, clicking on these links takes you to a fake website where you are asked to provide your personal details. The whole enterprise is a ploy to capture sensitive details, such as your email address and password, which the scammers then exploit at your expense.

Clickjacking for fake rewards

Here, the attacker tries to lure you into clicking a link by offering something in return, such as a free gift for completing a survey. However, when the link is clicked, it collects the details of whoever fills out the survey. This might include full names, addresses, phone numbers and email addresses. Scammers could use these to hack into your other accounts or simply sell your data to other criminals.

Malicious app downloads

Some cybercriminals design software that appears genuine or helpful (and is normally free) but has been created to steal your personal information. There may be a pop-up ad encouraging you to download and install the app. Once the app is downloaded, the attacker can see any personal credentials you enter, and could then use this information for their own gain.

'Payment first' scams

Prevalent on sites such as Depop, these scams have spread to Facebook since it added the Marketplace feature. A user lists an item for sale and requests payment up front. Most online stores work this way, but the crucial difference is that scammers ask for payment via PayPal friends and family – not goods and services. This means you can't dispute the payment: the scammer keeps your money, and you never receive the item.

Threats disguised as quizzes

Most quizzes on social media seem harmless, but many come with hidden threats. When you submit your answers, you're also agreeing to terms and conditions which – in some cases – allow the quiz developer to sell your details to third parties. This puts you at greater risk of phishing attacks and spam advertising emails. It might also give the app permission to use information from your profile.

Untrustworthy URLs

It's common on social media for URLs in posts to be shortened (to meet Twitter's character count, for instance). This may seem harmless, but it opens an avenue of attack for scammers who may be disguising a malicious link as legitimate. These links can install malware on the victim's device, which could lead to passwords being stolen or even be the precursor to ransomware attacks.

Angler phishing scams

Using a fake corporate social media account, the scammer pretends to be from customer services. When someone complains about customer service on social media, the fake account messages them asking for their name, phone number and email. If the user provides this info, they are directed to a fake website where they enter their login details. The attacker can then steal their credentials or infect their device with malware.

Advice For Parents & Carers

Set strong passwords

Always ensure that your passwords are not easily guessable. Try to use a mix of letters, numbers and special characters so that criminals cannot forcefully get control. You should also change your passwords every so often to provide further protection against your accounts being taken over. If you have any concerns about your account's privacy, change the password.

Review your privacy settings

Regularly review your privacy settings on social media. You can restrict which parts of your profile can be seen and by who. We recommended making your personal information only visible to friends, which will help to limit the information a scammer could find out about you from social media. It's also safest to only accept friend or follow requests from people that you actually know.

Protect your personal information

Never enter personal information on unfamiliar websites. If you were redirected to a site from a social media post or an email link, putting in your personal details could give key information away to a scammer. Fraudsters may pose as someone you know to try and get your address or bank details (or your family's). If this happens, block the user and tell your family, so the scammer can't try to deceive anyone else.

Avoid opening suspicious emails

When you get an email, always check the sender's address before opening it. If it's an unexpected email and the sender is a stranger, mark it as junk (in case they try again in future) and simply delete it. They could be a scammer who's simply seen your email address on your social media profile. Being aware of phishing attacks is the primary method of defence against scam emails like this.

Choose trusted download sources

Don't download apps or files from unknown sites – instead, use verified and trustworthy sources (such as Google Play or the App Store for download to mobile devices). You can recognise safe sources by their trust seals. The browser address bar on a secure site starts "https" instead of "http". A shield or lock symbol in the address bar also indicates that a site is secure.

Install anti-virus software

Another key tip is to ensure that you have robust and reliable virus protection installed on any of your devices that support it. Anti-virus programmes will help to insulate you against cyber-attacks by blocking any malicious downloads or detecting any recently downloaded malware and removing it. Update your virus protection software regularly and carry out frequent scans of your device.

Meet Our Expert

Formed in 2016, KryptoKloud provides cyber security and resilience solutions to its customers. With offices in the UK, the company offers managed service operational packages including cyber security monitoring and testing, risk audit, threat intelligence and incident response.

KryptoKloud

National Online Safety®

#WakeUpWednesday