

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
- ThinkUKnow Online Safety Packs
- Sharing Images
- Live Streaming
- Cyber Security

- Managing Social Media
- Coping Strategies
- Where to get support for your child
- Parents guide to Rocket League
- Parents guide to Social Media Scams

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 sale 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. Ty mutting 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.

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

火井*

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.



SCHOOL

MAIN ENTRANCE

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. NEWS

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 troils or bullies (or worse).





Online Safety









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:

Sharing images

Live streaming



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.

- 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.





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

fighting for young people's mental health

www.youngminds.org.uk/webchat

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...

OCKETLEAG

PEGI 3

18.

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



Unsuitable Online Interactions

Scams and **Bad Trades**

In-App Purchasing





Advice For Parents & Carers



Use Parental Controls

Monitor Gaming Time

It's impractical to sit and watch your child every time they play Rocket Loague. 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.

Stay Aware of Spending

Free-to-play games can become money sinks without children realising. For peace of mind, make sure you don't hav 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.

Encourage Regular Breaks

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

Meet Our Expert

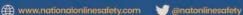




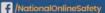
National Online Safetv #WakeUpWednesday

arental-Controls, nina.com/rocket-league/credit-system-free/











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 self-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 steel 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 so many the state of the state

Threats disguised as quizzes

Most quizzes on social media seem harmiess, but many come with hidden threats. When you submit your answers, your ealso 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 lake website where they enter their login details. The attacker can then stead their credentials or infect their device with malware.

Advice For Parents & Carers

Set strong passwords

Always ensure that your passwords are not easily guessable. Ty 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 accounts privacy, change the password.

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. Seling oware of phishing ettacks is the primary method of defence against scam emails like this.

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 salest to only accept friend or follow requests from people that you actually know.

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 bor 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.

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. Fraudaters may pose as someone you know to try and get your address or bank detail (or your family's). If this happens, block the user and tell your tamily, so the scammer can't try to deceive anyone else.

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 I. 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 2015, 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.





National Online Safety*







