



Tudor Grange Samworth Academy

Safeguarding Newsletter October 2020

Meet the Safeguarding Team



Peter Ephgrave
Designated Safeguarding Lead (DSL)



Rebekah Edwards
Deputy Safeguarding Lead



Anika Collins
Deputy Safeguarding Lead



Sue Perkins
Safeguarding Mentor (DDSL)



Maarya Alli
Safeguarding Support Assistant (DDSL)



Kerry Roberts
Deputy
Safeguarding Lead



Megan Nelson
Deputy
Safeguarding Lead



Kirsten Martin
Deputy
Safeguarding Lead



Terrie Roberts
Deputy
Safeguarding Lead

Welcome to our Parent Safeguarding Newsletter for this academic year. We will publish one each half-term with up to date news on safeguarding information to help you support your children.

All our safeguarding information is available on the school website at <https://www.samworth.tgacademy.org.uk/safeguarding/>

If you would like to contact a member of our safeguarding team please telephone the academy on 0116 2780232 or email safeguarding@samworth.tgacademy.org.uk

With so many students now having access to the internet and social media we wanted to make you aware the latest information and sites they may be visiting and how you can support.



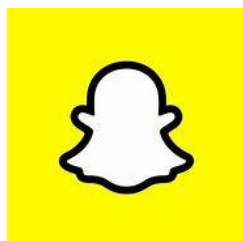
<https://onlyfans.com/>

The fast-growing social media platform stands out from the crowd through its focus on money: users pay a subscription to follow content creators, who in turn take home a large cut of that fee. It has become increasingly popular over the past few months, but that growth hasn't been without controversy.



<https://www.triller.co/>

Triller is the latest video sharing app on the market, which encourages users to create music videos and share them with the world. The platform boasts some of the music industry's biggest stars as users and recently announced that it had amassed over 250 million downloads worldwide.



<https://www.snapchat.com/l/en-gb/>

Snapchat – links to criminal groups

Another area of concern that appears to be on the rise in local communities is the use of Snapchat for criminal groups to send messages out for multiple users to see. These messages try to lure individuals in to try substances such as vapes which contain THC (Tetrahydrocannabinol is a cannabinoid which is identified in cannabis. THC is the principal psychoactive constituent of cannabis). They are even advertised as 'free' if the individual tries to get other individuals to try some, with the intended outcome of them all wanting more at a price. The criminal groups then drop these off in local community areas if a postcode is sent to them.

Trolling and online abuse

Trolling and online abuse are forms of cyber aggression that involve the sending of malicious, abusive or derogatory messages by one user (a 'troll') to another user online. Please see attached poster for more information and how you can support your children.

AT National Online Safety we believe in empowering parents, carers and educators with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. Please visit nationalonlinesafety.com for further guides, hints and tips for adults.

Part of our Online Bullying Series

NOS
Online Bullying

Brought to you by
NOS National Online Safety
www.nationalonlinesafety.com

What you need to know about... TROLLING & ONLINE ABUSE

What is it?

'Trolling & Online Abuse'

Trolling is a form of cyberaggression. It involves the sending of malicious, abusive or derogatory messages by one user (a 'troll') to another user online with the intention of upsetting or harassing them or damaging their reputation. It is often anonymous and does not meet the definition of bullying yet might develop into online bullying. Trolls will often goad others until they react. They enjoy putting people down and causing discord, starting arguments or being inflammatory – stirring things up for their own entertainment. Trolling may take the form of a one-off offensive comment, hate speech or even threats made online.

Know the Risks

May cause distress

Children can be particularly vulnerable to online trolling and online abuse. Receiving offensive comments for no reason can cause young people distress and increase feelings of anxiety and worry.

Impact on wellbeing

Trolling which is targeted and persistent can have a huge impact on children's mental health and wellbeing. It can lead to low self-esteem and create feelings of worthlessness and dissatisfaction, potentially affecting how children see and feel about themselves.

Could damage reputation

Online trolling can be humiliating for the victim and can negatively impact on how they are perceived online or on social media. Trolls might goad children into reacting or saying something they might regret and then sharing those comments widely to purposely paint them in a negative light.

May affect home and school life

Children who constantly receive hateful and spiteful messages online can become isolated and withdraw from daily life. They may become depressed, angry or unable to sleep at night. Their school performance may suffer and it may impact on their behaviour at home.

Safety Tips

Have open dialogue

It is vital to have conversations with young people about the hate speech, anger and prejudice that are all around them and explore what resilience they may have. Keep the dialogue always open so that young people have trusted adults to turn to.

Discuss online behaviour

Discuss what is acceptable behaviour online and what is inappropriate, unacceptable or against the law. Warn against reacting even more aggressively towards online trolls, reminding them that their digital footprint will outlast the current problem.

Implement privacy settings

Make sure that children are only using age-appropriate apps. Make their profiles private so that only friends and family can interact with them online and turn off comments if you're concerned about what other people might say.

Teach critical thinking

Help young people to spot trolls or when people are 'stirring it' on social media. Talk to them about people who might dare them to do risky things or encourage them to post negative comments online so that they recognise them and don't become an online troll themselves.

Further Support

Report to platform

Understand the tools available on the platform where trolling is taking place and whether or not it is moderated. Check out the community guidelines to see if the behaviour contravenes them and then if so, report it, block, unfriend or unfollow the sender where possible.

Collect evidence

Always try to screenshot or take a photo of the negative posts or comments made online. Report the incident to your child's school, police or local authority who will be able to investigate further.

Seek professional advice

If your child has experienced negative effects on their mental health and wellbeing due to trolling online, ask for additional support from your school's local safeguarding officer or seek professional help from charities who will be able to offer further advice and guidance.

Seek support from Friends

Friends can be supportive to one another and can be encouraged to flock to post positive messages when someone is targeted. Ask your child's friends for support – like-minded people can act together positively and they may help to build their confidence and self-esteem.

Our Expert

Adrienne Katz

Adrienne Katz is an award-winning cyberbullying expert with extensive experience of working with schools and education providers to deliver training in online safety. She is the founder and leader of the annual national Cybersurvey, providing one of the richest databases of young people's views on digital life in the UK and has previously worked on government level projects funded by the Home Office and The Princess Diana Memorial Fund.

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety Instagram - @nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 09.09.2020

Phishing

Phishing is the method of scamming users for their personal information online. Please see attached poster for more information and how you can support your children.

At National Online Safety we believe in empowering parents, carers and educators with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. Please visit nationalonlinesafety.com for further guides, hints and tips for adults.

Part of our Privacy & Security Series

What you need to know about... PHISHING

Brought to you by National Online Safety
www.nationalonlinesafety.com

What is it? 'Phishing'

Phishing is a form of cyber-attack where victims are targeted in the form of spoof emails, phone calls or texts. These are commonly carried out by an attacker posing as someone else to influence individuals into giving out sensitive data such as payment details and passwords. Phishing usually takes place via email, where the attacker manipulates a message to make it appear to be from someone else, therefore deceiving the victim into doing as they say. Hackers try to deceive you into downloading malicious code and will aim to extract small pieces of information at a time.

Know the Risks

- Loss of personal data**
If a young person has been the victim of a successful phishing attempt, hackers may gain access to their personal data and destroy/corrupt it. Some hackers may ask for a ransom in order to get files back, whilst others may simply destroy it or even publish it on the dark web.
- Targeted phishing**
If a hacker can trick children with a phishing attack, the chances are that they'll be back for more. They may begin asking for 'harmless' information, then move on to sensitive information such as passwords and entry codes. Many phishing attacks start with the attacker offering to help the victim with a common problem to build enough trust to ask for information such as passwords.
- Hidden entry**
If an attacker manages to successfully execute a phishing attack on a victim, they have essentially found a 'way in' or backdoor into their online security. Even if they do not notice any changes, the hacker may be monitoring/controlling their computer without their knowledge.

Safety Tips

- Backup your files**
Always create a backup of your files to an external hard drive or USB before any potential damage or destruction. If you regularly perform backups, you may only have to backup any files recently added/updated since the last backup.
- Disconnect the device**
If you think a child has been a target of a phishing attempt, firstly disconnect the device from the network by switching off the Wi-Fi in settings or unplugging the ethernet cable. Alternatively find the router and unplug it. This will prevent any malware from accessing any internet services.
- Scan your system**
Always perform regular and full malware scans; this will check for any potentially harmful programs installed on your computer. Scans are most effective when the antivirus is up to date so it's crucial to keep on top of the latest security downloads.
- Check official websites**
If you're unsure about a message you receive, don't click any links or follow any instructions. Check the official websites online and don't give out any personal information that you don't need to. Even if the message seems like it's from someone you know, if anything seems suspicious, or matches any of the criteria above, simply do not open it...

Look out for...

- Suspicious URLs**
Sometimes links and attachments aren't always what they appear to be and could send you to a site completely different to what was expected. Hovering over a hyperlink will display the actual website. Some links are shortened, so the actual website address is hidden behind a generic link, such as goo.gl/7h28. Never click shortened URLs.
- Odd sense of urgency**
Cyber criminals will put fear in their victim's mind in an attempt to push them into giving away personal information. They may act as if they're trying to help create a false sense of 'trust' or pressure users into giving information 'before it's too late'.
- 'Too good to be true'**
If you receive an email saying you've 'Won a new phone' or a 'Holiday Abroad', it's likely to be a phishing email. Hackers engineer emails and trick targets into believing they've won something, as it puts a false sense of trust towards the hacker.

Our Expert Emma Davis

Emma Davis is a cyber security expert and former ICT teacher. She delivers cyber awareness training to organisations nationally and has extensive knowledge and experience of managing how children access services and apps online.

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety Instagram - @nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 12.08.2020

Webcams

The use of webcams has become hugely popular since the start of the coronavirus pandemic. Widely used on popular apps such as Zoom, Skype or Microsoft Teams, they provide users with the ability to take part in video calls and actually see who they're speaking to. Whether used for remote learning, home working or just keeping in touch with family and friends, webcams have been crucial to helping all of us keep in touch. Please see attached poster for more information and how you can support your children.

At National Online Safety we believe in empowering parents, carers and educators with the information they need to hold an informed conversation about online safety with their children, should they feel it is needed. Please visit nationalonlinesafety.com for further guides, hints and tips for adults.

What you need to know about... WEBCAMS

Part of our Privacy & Security Series
NOS Online Privacy & Security
Brought to you by
NOS National Online Safety
www.nationalonlinesafety.com

What are they?

'Webcams'

Most commonly found embedded in laptop screens and smartphones, webcams are tiny video/still cameras designed to let you participate in video calls on services such as Skype and Zoom. They have become hugely popular since the start of the coronavirus pandemic, allowing homeworkers to chat with remote colleagues and helping friends and families stay in touch. However, there are many security and privacy risks associated with webcams that owners should be aware of.

Know the Risks

Hackers

Webcams are a prime target for hackers as they give attackers a highly intrusive eye into the victim's home. There have been several high-profile breaches where integrated laptop webcams or dedicated webcams have been targeted.

Malware

Malware often targets webcams, secretly giving hackers access to your computer's webcam without any visible signs that the camera is switched on. Such malware can arrive in email attachments or by clicking on rogue links on websites, and it can often install itself in the background without the user being alerted.

Access to strangers

Children can be naive to the dangers of allowing strangers to access the computer's webcam. They may click through warning messages that grant access to the camera or they may willingly share the camera with people they meet online who are pretending to be children.

Blackmail

Webcams can be used for blackmail, even when the webcam itself hasn't been hacked. Fraudsters will claim to have webcam footage or stills of the victim whilst naked or accessing pornography and threaten to post such footage on social media or send it to employers if the victim fails to pay up. The fraudsters normally don't have any footage at all, but the threat is often enough.

Look out for...

The indicator light

It can be difficult to tell if your webcam has been compromised or is secretly capturing footage. If the little indicator light (normally green) next to the webcam is lit when you don't expect it to be, this could be a sign.

Camera permissions

Check the camera permissions on your computer to ensure no rogue or unnecessary apps have been granted access to the camera. Switch off any apps that don't need access to the camera. If you never use the webcam, you can bar all access to the webcam. Better still, cover it when not in use.

Unexpected saved folders

Another telltale sign of a webcam compromise is folders containing videos or photos taken by your webcam appearing on your computer. Malware will often save videos/photos on your machine before attempting to upload them to the hackers, who will then use them for blackmail purposes. Check your Photos and Videos folders occasionally for any unexpected files.

User Safety Tips

Explain the dangers to children

Talk to your children about the dangers of talking with strangers via webcam and tell them not to accept any video chat requests from people they don't know in real life. Keep computers in family rooms, so that children can't covertly use the webcam in their bedrooms.

Refuse & report

Do not pay anyone claiming to have captured embarrassing webcam footage of you. It's highly likely they don't have footage in the first place, and even if they do, paying them may encourage them to demand more money. Report the matter to the police and keep a record of any evidence you can.

Unplug webcams & update firewalls

Unplug external (USB) webcams when they're not in use. Make sure your computer is running up-to-date security software and that the firewall is switched on. This can thwart attempts to access your webcam remotely.

Our Expert

Barry Collins

Barry Collins has been a technology journalist and editor for more than 20 years, working for titles such as The Sunday Times, Which?, PC Pro and Computeractive. He's appeared regularly as a technology pundit on television and radio, including on BBC Newsnight, Radio 5 Live and the ITV News at Ten. He has two children and has written regularly about internet safety issues over the years.

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety Instagram - @nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 05.08.2020

Sexting

Sexting, or sending nudes, is illegal for anyone under the age of 18. Despite this, recent research suggests that young people continue to share nude images of themselves, with one in five teenagers admitting they were pressured or blackmailed into it. Separate research also indicates an increase in so-called 'sexts' typed out by children during lockdown. Please see attached poster for more information and how you can support your children.

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

What parents need to know about

SEXTING

18+

Sexting involves sending, receiving or forwarding explicit messages, images, or videos of a sexual nature. Although mobile phones are the most common vehicle for sexting, the term can also apply to sending sexually explicit messages through any digital media such as email, instant messaging, and/or social media sites. They can be sent to or from a friend, boyfriend, girlfriend, or someone your child has met online. Sexting is often described as the new flirting for children, but it is illegal for anyone under the age of 18. Some of the main platforms it occurs on are Snapchat, Tinder, WhatsApp, Facebook Messenger, Instagram and Kik.

IT IS ILLEGAL

Sexting is illegal if you share, make, take, or distribute an indecent image or video of a child under the age of 18. It is an offence under the Protection of Children Act (1978), the Criminal Justice Act (1988), and under section 67 of the Serious Crime Act (2015). Sexting or 'youth produced sexual imagery' between children is still illegal, even if they are in a relationship and any images are shared consensually.

PERCEIVED AS 'BANTER'

Many young people under 18 see sexting as 'banter' and an easy way to show someone that they like and trust them. Whilst it is a criminal offence, the reasons for taking and sharing can be very innocent and all part of growing up, understanding their own sexuality, and establishing a relationship. However, whilst most images and videos are taken and shared willingly, there can be unintentional consequences, embarrassment, humiliation, and emotional hurt.

ONLINE BLACKMAIL OR BULLYING

Sexting can also expose young adults to the risk of being exploited by paedophiles or sexual predators, who then use images to extort additional photos, sexual favours, and sometimes money from victims. Your child may also feel pressured into sexting so they don't come across as boring, or think it's a way to show someone they care for them. They may feel under pressure to give in to repeated requests or feel obliged to share sexual messages and imagery which could then be used against them as a form of bullying or intimidation.

FEELINGS OF REGRET

Although some children willingly exchange messages, images, or videos, many may regret sharing them after they've been sent. Once it's out there, there's no going back and your child may feel ashamed, vulnerable, or anxious about the imagery resurfacing later, especially if a relationship or friendship has broken down.

NO CONTROL

Once a photo or video is out there, there's no way of knowing how many people have saved it, tagged it, or shared it. Children like to show off to their peers and, suddenly, an image has gone beyond its intended recipient to classmates, friends, and even strangers. Once an image or video has been shared online, there's nothing to stop it being archived and repeatedly shared.

Safety tips for parents

18+

THINK ABOUT LANGUAGE USE

Teenagers often prefer to use the word 'nudes' to 'sexting'. One reason for this is the normalising of this behaviour; another is that most children always feel a sense of embarrassment when discussing any issue with the word 'sex' in it. Sexting an image could also be described as an 'inappropriate selfie'. Using this term with your child might make the discussion less embarrassing.

BLOCK & PARENTAL CONTROLS

Show your child how to use the block button on their devices and favourite apps to stop people sending them unwanted messages. You can also set up parental controls with your internet service provider or on your child's phone to stop them from accessing harmful content.

EXPLAIN THE REPERCUSSIONS

Let your child know that once they have sent a message, they are no longer in control of it and the messages, images and videos that they may intend to share with one individual may end up where the whole world can have access to them. Even if they completely trust someone, other people using their phone might accidentally see it. And, later in life, it may affect their online reputation, especially if universities, employers or future partners access the imagery.

TALK TO YOUR CHILD

Encourage open dialogue about appropriate information to share with others, both online and offline. Show that you understand that sexting can be about finding out about nudity, bodies and exploring their sexuality, but explain why it's important to think twice before sharing something. Show that you are approachable and understanding and discuss what a healthy and trusting relationship with a partner looks like.

DISCUSS THE LEGALITIES

Children and young people may not realise that what they are doing is illegal. Ensure that your child understands that when they are aged under 18, it is against the law for anyone to take or have a sexual photo of them - even if it is a selfie and even when the activity is consensual.

LEARN HOW TO RESPOND

If an image has already been shared, either your child or you should speak to the person that the image was shared with and ask them to delete it. You can also use the report button on a website where the image was posted. Speak to your child's school as they may be able to confiscate phones if they know that they have sexual imagery stored. If you believe the child was forced into sending the message, report this to the police. You or your child can also report the content to a child protection advisor at the CEOP.

Meet our expert

Jonathan Taylor is an online safety expert and former Covert Internet Investigator for the Metropolitan Police. He is a specialist in online grooming and exploitation and has worked extensively with both UK and international schools in delivering training and guidance around the latest online dangers, social media apps and platforms.

www.nationalonlinesafety.com Twitter - @natonlinesafety Facebook - /NationalOnlineSafety Instagram - @nationalonlinesafety

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 15.07.2020

What parents & carers need to know about...

TRILLER

12+

Triller is a social media video sharing app. Unlike TikTok and many other video sharing apps, Triller focuses more on making creative music videos. Users can film multiple takes of themselves and the app will then automatically compile the best clips and turn it into a music video. It is free to download and has amassed over 250 million downloads worldwide, including celebrity users such as Justin Bieber, Eminem and Alicia Keys.

Default to Public Profile

When signing up to Triller your account automatically defaults to public. This means that any videos that your child uploads to Triller can be searched for and viewed by anybody who uses the app. It also means that anybody can send them a follow request or comment on their videos, including people they have never even met or seen before.

Drive for 'fame'

Verified users in Triller can exchange their Gold for Gems which in turn can be exchanged for real cash. Verified users are those that have gained enough likes and followers on the app, which could push some children to create more outrageous, dangerous or even inappropriate content in order to get noticed and earn more gold from their 'supporters'.

Unauthorised sharing

Once a video is uploaded and posted on Triller, it can be shared further by other users. Viewers can choose whether to share it on other social media channels, via email, messaging apps or even opt to download and save it to their device. This means anybody could potentially view, store and share your child's videos without you knowing or your consent.

Lack of privacy protection

Triller reserves the right to use anything publicly distributed on the platform for marketing and/or commercial purposes. That means that any content produced on the app which is available to the public can be used by Triller to promote themselves, even if you don't want them to.

In-app purchases

Gold coins are the currency in Triller and can be purchased in the app with packages ranging from \$0.99 to \$99.99. The money can be used to donate or 'support' other users who children follow and find engaging. This could mean that some children quickly rack up hefty bills if they have access to payment methods and are easily influenced by who they follow online.

Risk of cyberbullying

Triller gives users the ability to comment on other people's videos, even if they don't follow that account. Most comments are usually displays of positive feedback and showing appreciation for the content. However, if children post their videos in public, they could be at risk of online trolls posting hurtful or negative comments or become the victim of online bullying behaviour.

Mature content

Triller does contain references to more adult themed content. This includes bad language and references to drugs, alcohol and sex. The app has an age-rating of 12+ however there are no content filters and children can search for almost anything. Furthermore, users don't need an account to view other videos on Triller which means that children could use the app without having to sign up.



Safety Tips

Make accounts private

There aren't many parental controls on Triller, however users can make their profiles private which means only people your child approves can view and comment on their videos. It also means that your child will need to approve a request if somebody wants to follow him/her.

Talk about personal data

It's important to talk to your child about protecting their personal information online. Encourage them to only share their videos with friends and family that they also know and trust offline, and to avoid linking their other social media accounts to the platform.

Block and report strangers

If your child is receiving negative comments or is being harassed, you can report and block a user within the app. You can do this by going into the profile page of the other user. Make sure your child knows to never allow a stranger to follow them and to always come to you if they're ever unsure about someone who tries to contact them.

Discuss content concerns

Encourage your child to talk to you if they have seen a video on the app that has made them feel uncomfortable. Inappropriate content can be reported to Triller so it's important children know what is and isn't acceptable online. Talk to them about what they watch and who they follow. Try to get them to think critically about the things they see so that they can make better decisions online.

Remove payment options

Remove any links to payment options on your child's devices or enable payment monitoring controls. This will prevent them from making in-app purchases and spending money freely. If your child wishes to donate to a particular user, ask them questions around why they think that user needs the donation and whether they are real with their request. Remind your child that not everything they see online is the truth and they could be trying to fool them.

Explore yourself

The best way to understand the content on the app and how it works is to use it yourself. Follow your child's account so that you know what they are viewing and sharing online. Explore different videos and understand how the app works so that if your child has any concerns, you can support them with confidence.

Meet our expert

Parveen Kaur is social media expert and digital media consultant who is passionate about improving digital literacy for parents and children. She has extensive experience in the social media arena and is the founder of Kids N Clicks, a web resource that helps parents and children thrive in a digital world.



Resources are available from the national online safety organisation and are excellent and we use them as an academy to support the work we do with the student in school.



<https://nationalonlinesafety.com/>