The Acorns School

SPRING TERM EDITION 2023

Online Safety

Welcome to the first edition of The Acorns School Online Safety newsletter. As a school, we want to keep parents and guardians up to date with any changes that we think are useful in order to keep our students safe online.

Social networking is hugely popular. Many young people are sophisticated in the way they use social media apps and websites, tailoring their communication for different audiences, and accessing them from a range of devices including smartphones, tablets, and game consoles. Social media, like all forms of public communication, comes with some risks. Not all of these risks turn into actual problems; and if children never face any risks, they never learn how to deal with them. By helping your child understand what the risks are, you can play a big part in preventing them from turning into problems.

Understand the risks children may need to deal with

- Seeing or sharing of violent, sexual and pornographic content
- Inaccurate or false information and extreme views
- Promotion of harmful behaviours including self-harm, anorexia and suicide
- Over-sharing of personal information

Website:	Contact:	Email:
🔗	☎	✉
https://theacornsschool.co.uk	01695 575 486	admin@westlancspcss.lancs.sch.uk

- Actively or unintentionally getting involved in bullying or hurtful behaviour
- People who might bully, intimidate or frighten
- People posing behind fake profiles for: Mischief-making/Sexual grooming and stalking/Blackmail and extortion/ Identity theft and hacking

WhatsApp

To better secure your WhatsApp account, follow these tips:

- Never share your registration code or two-step verification PIN with others.
- Enable two-step verification and provide an email address in case you forget your PIN.
- Set a voicemail password on your phone that's difficult to guess to prevent anyone from accessing your voicemail.
- Check your linked devices regularly. Go to WhatsApp **Settings** > **Linked Devices** to review all devices linked to your account. To remove a linked device, tap the device > **Log Out**.
- Set a device code and be aware of who has physical access to your phone.
- **Note**: If you receive an email to reset the two-step verification PIN or registration code but didn't request this, don't click on the link. Someone could be trying to access your phone number on WhatsApp.

TikTok

To better secure your Tik Tok account, follow these tips:

- Use a strong password by combining upper and lowercase letters, numbers and symbols
- Don't use the same password across multiple sites or apps
- Make your password longer and more complex (you might also consider using a password management tool)

Be thoughtful about the info you put in your profile. Even with a private account, your profile information (including profile photo, username and bio) will be visible to all users. So while it's a good idea to avoid including things like your city or other identifiers, there's plenty of other ways to express yourself in your profile. Think about options like:

- A quote or song lyrics
- Hashtags or emojis
- Your favourite hobbies or sports

Choosing a public or private account
Whether you want to share your videos with the world or just your closest friends, the choice is up to you.
By default, your account starts as public, which means any TikTok user can view your videos and

post comments, reactions, or duets to engage with the content you've created and shared—but you can easily change this in your Privacy Settings.
If you switch to a private account you can approve or deny follower requests and only users you've approved as followers can see your content.
Whether you have a public or private account, anyone can choose to make a specific video private. Private videos are visible only to you and you can select this setting when you originally upload the video or later by making an uploaded video private. Remember, You may not use TikTok if you are under 13.

Snapchat

- Never share your password with anyone — not even us! A Snapchat representative will never ask you for your password. We don't need it to help you.
- Check Your Privacy Settings to choose who can send you Snaps, view your Stories, or see your location on Snap Map.
- Choose a Strong Password
- Verify Your Email and Mobile Number
- Set up Two-Factor Authentication
- Keep it Between Friends-Snapchat was made for keeping in touch with your close friends. We recommend that you only accept friend requests from people that you know in real life.
- Report Abuse on Snapchat

Instagram

There are several things that you can do to help keep your account safe:

- Turn on two-factor authentication for additional account security.
- Never give your password to someone you don't know and trust.
- Think before you authorise any third-party app – you should never share your login information with an app that you don't trust. If you give these apps your login information, whether with an access token or by giving them your username and password, they can gain complete access to your account.
- Pick a strong and unique password that you haven't used for other accounts. Use a combination of at least six numbers,

- Customise Your Location on the Map. Only the people you choose can see your location
- Change Who Can View My Story. The default privacy setting is that only Snapchatters you've added can view your Story.
- Don't Forget About Screenshots. Snaps are designed to delete by default, but people that you send Snaps to can still take a screenshot or take a picture of the Snap with another device, so it's a good idea to think before you share.

The Family Centre on Snapchat helps parents get more insight into who their teens are friends with and who they have been communicating with, while still respecting their teens' privacy and autonomy. It's designed to reflect the way parents engage with their teens in the real world, where parents usually know who their teens are friends with and when they are hanging out, but don't eavesdrop on their private conversations. Family Centre will provide parents over the age of 25 the ability to:

- See which Snapchat friends their teens have sent messages, photos or videos to in the last seven days, in a way that still protects their privacy by not revealing the actual contents of their conversations (Snaps and messages);
- See a complete list of their teens' existing friends, and allow parents to easily view new friends their teens have added, making it easy to start conversations about who their new contacts are;
- Limit their teen's ability to view certain content in the Stories and Spotlight tabs
- Easily and confidentially report any accounts parents may be concerned about directly to our 24/7 Trust and Safety team

letters and special characters (such as !$@%), and try to avoid repetition.

- Change your password regularly, especially if you see a message from Instagram asking you to do so. During automated security checks, Instagram sometimes recovers login information that was stolen from other sites. If Instagram detects that your password may have been stolen, changing your password on Instagram and other sites helps to keep your account secure and prevents you from being hacked in the future.
- Make sure that your email account is secure. Anyone who can read your email can probably also access your Instagram account. Change the passwords for all of your email accounts and make sure that no two are the same.
- Download your data. You can keep a backup of your data by requesting a copy of everything you've shared on Instagram in a machine-readable HTML or JSON format. Note: You'll need your Instagram account password to request this information.
- Log out of Instagram when you use a computer or phone that you share with other people. Don't tick the "Remember me" box when logging in from a public computer, as this will keep you logged in even after you've closed the browser window.

For more information, you can find out how children use social media, the apps they use, the risks they face, how to use privacy settings, and advice and tips about how to talk to your children at:

• www.childnet.com/sns
• www.internetmatters.org
• www.nspcc.org.uk/onlinesafety
• www.parentzone.org.uk
• www.thinkyouknow.co.uk/parents
• www.askaboutgames.com

If you are concerned about online grooming or sexual behaviour online, contact CEOP: www.ceop.police.uk
If you stumble across criminal sexual or obscene content on the internet you should report it to the Internet Watch Foundation: www.iwf.org.uk

Work through safety and privacy features on the apps that your child is using, or might use. Make sure they understand the point of these and how to use them. Don’t be put off by believing your child knows more than you: the tools are actually quite easy to manage.

• Ask them to show you which social media apps they use and what they like about them. Talk about how they use them and what makes them so engaging.

• Explain how you can use privacy settings to make sure only approved friends can see posts & images.

• Check if any of their apps have ‘geo-location’ enabled, sharing their location unintentionally.

• Show them how to report offensive comments or block people who upset them.

• Check ‘tagging’ settings so that when others are posting or sharing photos online, your child’s identity is not revealed. Also, get people‘s consent before sharing photos.

• Encourage your child to come and talk to you if they see anything that upsets them

Website:	Contact:	Email:
https://theacornsschool.co.uk	01695 575 486	admin@westlancspcss.lancs.sch.uk

In a mobile age, children can't be completely protected, even by the best privacy controls; another child may use different settings. So it's important to keep talking to your child about the implications of social media. Getting a sense of what they think is a useful place to start; you may be surprised by how much thought they may have given to the issues. Encourage your child to think carefully about the way they, and others behave online, and how they might deal with difficult situations.

- People may not always be who they say they are online: how can this create problems?

- Why is it unwise to meet anyone in the real world that you've only ever met online?

- Even if you think your messages are private, remember that words and images can always be captured and broadcast.

- People present themselves differently online - do they really look like that? Are they always having that good a time?

- Be aware that screens, and especially being anonymous, can lead people to say things they wouldn't say to someone's face.

- What does being a good friend and a likeable person online look like?

- There can be pressure to be part of a particular group online or to be seen to be following a certain set of ideas. How can you take a step back and make your own decisions?