Weston St Mary CE Primary School

Online Safety Newsletter January 2026

Instagram Teen Accounts - update

You must be over 13 years of age to set up an account. Instagram is used to post photos and videos as well as send direct messages, make voice/video calls, and send disappearing messages.

Teen accounts are automatically set up for users aged 13 – 17. Instagram have announced that teens will now see content similar to content that they would see in a PG-13 movie.

Instagram have also updated their policies around content to include "hiding or not recommending posts with strong language, certain risky stunts, and additional content that could encourage potentially harmful behaviors"

Finally, for parents who would like to apply more stringent settings, Instagram are also introducing a new, stricter setting called 'Limited Content.' This setting will mean your child is not able to see, leave, or receive comments under posts as well.

You can read about the updates here: https://about.instagram.com/blog/announcements/instagram-teen-content-safety-pg-13

Playing games online

Does your child play games online? We have outlined some risks that you should consider:

Chatting to strangers / risk of inappropriate language

Some games will allow communication via text chat, direct messages or chatting. Some games do offer the ability to switch communication off and/or the option to restrict bad language, so make sure settings appropriate to your child are applied. If your child is playing online with strangers, then you need to be aware that there is a risk of grooming. Some games do allow you to restrict communication to 'friends only,' however you would need to monitor that their online friends are real life friends. It can be difficult to moderate online chat so ensure your child knows how to block and report other players.

Cyberbullying

It can be very easy online for children to behave in a way that they would not if they were face to face. Talk to your child about how they speak to others online and encourage them to talk to people online with respect. Other forms of cyberbullying whilst playing games could be excluding others, criticising the ability of other players and ganging up on others.

In app purchases

Many games include the option to purchase additional items/ subscriptions so ensure you do not have payment cards saved or set up restrictions/ a password to approve purchases.

What can I do?

- **Set up parental controls** - as well as setting up appropriate parental controls through the game's settings, ensure you have set them up on the console/device your child is playing on.
- **Check age ratings** - before buying the game, check that your child is old enough to play it. All games will either have a PEGI rating or be rated by the App Store/Google Play.
- **Chat to your child regularly** about the risks above so that they are aware of what can happen online and remind them to always talk to you or a trusted adult if they have any concerns

Further information

CEOP provides further guidance and support regarding this topic: https://www.ceopeducation.co.uk/parents/articles/gaming/

Snapchat

Snapchat is a popular social media app used for messaging and sharing photos and videos. **You must be 13+ to sign up.** Users can send messages (snaps) to others that are only seen for a set time, and users can also upload snaps to stories, which disappear after 24 hours.

Key Concerns

There are potential risks such as:

- the risk of your child viewing content that is not appropriate for their age.
- location sharing (via Snap Map).
- cyberbullying.
- contact from strangers.
- excessive screen time – children may have a fear of missing out (FOMO) as well as pressure to maintain "streaks".
- "disappearing" messages can lead to more risky behaviour and a "false sense of security." These messages could be screenshot or another device used to take a photo, so they're not actually deleted as the sender believes. The image could then be shared.
- in app purchases.

Parental Controls / Safety settings

Snapchat's Family Centre is a set of parental controls and includes tools such as allowing you to:

- see who your child is friends with.
- see who your child has sent messages (not the contents of conversations though), photos or videos to in the last week.
- view a list of group members for groups that your child has been active in.
- restrict content to limit access.
- report any accounts that you are concerned about.

You can learn more about Family Centre here:
https://parents.snapchat.com/parental-controls?lang=en-GB

If your child is using Snapchat, then make sure the appropriate privacy settings are set up, including who can see their location and who can contact them. Also ensure your child knows how to block and report other users if necessary:
https://help.snapchat.com/hc/en-gb/articles/7012343074580-How-do-I-change-my-privacy-settings-on-Snapchat

More information

For more detailed advice and information:

- https://parentzone.org.uk/article/snapchat
- https://parents.snapchat.com/safeguards-for-teens

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date released 01.01.26. The inclusion of any links does not imply any affiliation with or endorsement of the linked websites, documents, or videos, nor are we claiming any ownership

Family Smart Start

Family Smart Start is a free toolkit designed to help you and your child navigate the milestone of getting their first phone. The toolkit provides support on how to set up their new phone, how to talk to your child about digital safety and a template family agreement. Find out more here:

https://familysmartstart.com/

Cyber security

Cyber security is the process of protecting your information and data whilst online against scams and cyber-attacks. Cyber-attacks are the process of maliciously targeting individuals or organisations to disable networks or steal data for example.

The National Cyber Security Centre (NCSC) have an area on their website with guidance to help protect you and your family. The guidance includes how to manage your digital footprint online, information about anti-virus software as well as top tips for staying online such as:

- Using a strong password
- Setting up 2step verification

You can find the resources here:

https://www.ncsc.gov.uk/section/advice-guidance/you-your-family

The NCSC also provide advice on what you should do if you are the target of a scam or cyber-attack. Find out more here:

https://www.ncsc.gov.uk/section/respond-recover/you

Would you like to read this newsletter in a different language? You can use the translate tool on our web version: https://www.knowsleyclcs.org.uk/january-2026-primary/