



Online Safety

June 2025

Virtual Reality (VR)

VR is a 3D computer generated environment that users can explore wearing a VR Headset.

Meta Quest Parental Controls

Meta Quest are one of the more popular VR Headsets. Users aged 13+ can use Meta Quest (children between 10 and 12 years old can use it through a parent managed account). *Meta Quest state that VR Headsets are not recommended for use by younger or smaller-sized children for a variety of reasons including eye strain.* Optional supervision tools are available for those aged 13–17. Find out more here: <https://familycenter.meta.com/uk/our-products/horizon-and-quest/>

Meta Quest has a Safety Centre; it includes health and safety warnings and how to set privacy settings. <https://www.meta.com/gb/quest/safety-center/>

Gorilla Tag

This is a popular game and whilst rated as PEGI 3 (even though young children should not be using VR), it is important to note that it does include in app purchases and players can interact so there is a risk of offensive/inappropriate language. <https://www.esrb.org/blog/a-parents-guide-to-gorilla-tag/>

What can I do?

- Check what games your child is accessing and make sure they are appropriate.
- Play together.
- Set time limits and ensure plenty of breaks.

Further information:

- <https://www.nspcc.org.uk/keeping-children-safe/online-safety/virtual-reality-headsets/>

Online Privacy

It is important to develop an understanding of how you can protect your child's privacy online. Any personal information shared online creates a digital footprint and it is vital that we control who sees what.

What are Privacy settings?

Privacy settings are tools available on most social media apps, websites, and games. They allow users to control who can view what they share online.

What can we do to support our children with their online privacy?

Talk to your child regularly: Talk to your child about what is personal information and to think about what they share online. Personal information includes their name, address, current location and the school they attend. This also includes information within photos or videos that they may share, for example does it show their current location?

Apply appropriate privacy settings: For any app, game or device that your child uses, check the privacy settings and apply them as appropriate. For example:

- Check if their location is being shared.
- Check who can tag them in posts (as what others tag them in can also affect their digital footprint).
- Check who can share their content.

Check these settings regularly as new options may become available or sometimes updates can change previous settings.

Children learn from us: Think about what you are sharing online – do you share photos of your child in their school uniform or their current location?

Set strong/complex passwords: Teach your child to create strong/complex passwords and to never share them with others.

Search their name – search their name in a search engine to see what information can be seen about your child. Remind your child that they can delete any information that they no longer want others to see.

Further Information

- <https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/taking-care-your-digital-footprint/>
- <https://www.unicef.org/parenting/child-care/online-privacy>
- https://www.ceopeducation.co.uk/11_18/lets-talk-about/online-safety/privacy-settings/

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date released 01.06.25. 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 or copyright in the content of the linked materials.



Instagram

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. Users can also upload to 'Stories' (which disappear after 24 hours), broadcast live and upload reels (short videos).

Teen accounts

Teen accounts are automatically set up for users aged 13 – 17. Teens under the age of 16 will need your permission to update their safety settings. With a Teen Account, additional safety settings are applied, for example, who your child can contact is limited and the content they access will be set to the most restrictive setting to reduce exposure to sensitive content. Find out more here: <https://help.instagram.com/995996839195964>

Supervision settings

Instagram also offers a supervision facility, which is a set of tools that you can use to help support your child. It is important to note that both you and your child must agree to these settings, and they can be removed at any time by either person. Once set up you can:

- Set a time limit.
- See which accounts your child is following and who is following them.
- View who your child has messaged in the past week (you will not be able to see the contents of these messages)
- The option to block your child from accessing Instagram at certain times e.g. during school or at night.

Find out more here:

https://help.instagram.com/658522825492278/?helpref=related_articles

How to Reset Your Instagram Recommendations

You can reset recommendations, which will clear recommended content across Explore, Reels and Feed. You can find out more here: <https://about.fb.com/news/2024/11/introducing-recommendations-reset-instagram/>

What are the risks of using Instagram?

- Cyberbullying.
- Risk of contact from strangers.
- Viewing inappropriate content.
- Echo chambers - algorithms can create an echo chamber. Once we show an interest in a subject, the app/ site will promote that content, which may mean we are overly exposed to it.

Safety Features

If your child is using Instagram, then ensure they know how to report posts and people, how to unfollow/block people as well as delete and turn off comments. Find out how: <https://help.instagram.com/269765046710559>

More information

Visit the family centre to learn more about the features available: <https://familycenter.meta.com/uk/>

Talking to your child about online mistakes

The online world is difficult to navigate, and mistakes will happen. When they do, it is important that as a parent you are ready.

Stay Calm

If your child tells you about something that they have done wrong online, then try to stay calm and listen.

Be Honest

You may not know how to solve the issue but tell them you will help them work it out.

Solve It Together

Try and resolve the problem together to help your child learn and understand what went wrong. This will also develop their digital literacy skills.

You should also take the opportunity to review/set up any available parental controls.

Help and Support

If you feel like you need support from an external organisation, then Parent Zone have listed some of the different organisations available: <https://parentzone.org.uk/article/help-and-support>

Further information:

<https://www.brightcanary.io/what-to-do-when-your-child-sends-inappropriate-things/>

Texting dictionary from Internet Matters

Internet Matters have created a list of text language terms to help you understand some of the text slang that your child might be using. Find out more here:

<https://www.internetmatters.org/resources/text-dictionary/>