



Cyberflashing

Supporting victims of cyberflashing and giving preventative advice.

76% of girls aged 12-18 have been sent unsolicited nude images of boys or men*

‘Cyberflashing’ is where somebody digitally sends sexual images or pornography to an unsuspecting person. Due to the nature of channels used to send these images, the victim will not know they have been cyberflashed until they have actively opened the notification or gone into the app.

AirDrop is a file and image sharing app, bespoke for Apple devices, which enables users to drop content for nearby devices to accept or reject. Cyberflashing most commonly occurs using Apple AirDrop, as strangers can send images to a victim’s phone without having their details saved. Cyberflashing can also occur through **file sharing apps** and **social media**, especially if the perpetrator has the victim’s details.

Best practices for parents and carers (preventative):

Discuss boundaries and encourage open communication

Tell your child that their boundaries are valid and that if anything breaks those boundaries – whether strangers inside or outside of school; or even close friends or partners – then they should speak to you or a trusted adult about it straight away. Make sure that they know you will support them without judgement no matter what happens.

Check your child’s AirDrop settings

If your child has an iPhone, check their AirDrop settings with them (Settings > General > AirDrop) and, if necessary, take a look at their privacy settings. The default is set to “Everyone”, meaning anyone nearby can send unsolicited photos straight to your child’s phone. We recommend switching to “Contacts Only” so that only friends can send photos, or even “Receiving Off” if you and your child decide this is the safest option for them.

Establish safety features of other apps

Cyberflashing still occurs through social media and file sharing apps when privacy and safety features have not been enabled. Look through your child’s apps with them and set privacy settings to “friends only”; be selective about who can follow them or they can follow.

Best practices for parents and carers (if your child is a victim of cyberflashing):

Keep calm and praise them for approaching you

It can be very difficult for a child to speak up about things which they perhaps don’t fully know about or which they may find embarrassing. They may have gone through a lot of anxiety and worry to bring it up with you, so make sure you insist that they have done the right thing and that none of it is their fault.

Assess the situation and report



If this has happened at school, you may want to contact your child's school, as their safeguarding policies will allow them to escalate and deal with the situation. If this has happened with a perpetrator outside of school, in public, it can still be worthwhile to seek support from the school, or you may want to consider calling the local police.

Change your child's phone settings

If your child has an iPhone, check their AirDrop settings with them (Settings > General > AirDrop) and switch the default from "Everyone" to "Receiving Off", or at least "Contacts Only".

Seek help from the professionals

Make sure your child is aware of the support available for victims.

Provided by the UK Safer Internet Centre and operated by [SWGfL](#), [Report Harmful Content](#) is a national reporting centre that has been designed to assist anyone in reporting harmful content online, as well as offering guidance and mediatory support to victims. [The Mix](#) is a charity which provides free, confidential support for young people under 25 via online, social and mobile.

How to teach young people about cyberflashing

Talk about healthy relationships and consent

Let your child know that boundaries are subjective and personal; other people's opinions should be respected. Empowering them to take action if they are being pressured will help to build their confidence.

Have an open conversation

Allowing for discussion is essential in gauging the variety of your child's opinions, and offers a chance for you as an adult to mediate conversation.

Defining online sexual harassment

26% of 13-17 year olds have had rumours about their sexual behaviour shared online in the last year, with 65% saying that girls are judged more harshly for this than boys.

47% of 13-17 year olds have witnessed their peers editing photos of someone to make them sexual e.g. placing sexual emojis over them or adding different faces to pornographic images.

31% of 13-17 year olds have seen their peers create fake profiles of someone they know to share sexual images, comments or messages.

Online sexual harassment is **unwanted sexual conduct** on any digital platform and it is recognised as a form of sexual violence.



Online sexual harassment encompasses a wide range of behaviours that use digital content (images, videos, posts, messages, pages) on a variety of different platforms (private or public).

Online sexual harassment can affect children and young people in many ways—from unwanted messages and inappropriate comments to pressure for images or private conversations. As a parent or carer, your awareness and support play a crucial role in keeping your child safe.

What parents should know

- **It can happen anywhere online:** social media, gaming platforms, messaging apps, and online forums.
- **It often starts subtly:** messages may begin as friendly chats before becoming inappropriate or uncomfortable.
- **Children may not always recognise it** or feel confident to speak up, especially if they feel embarrassed, worried about getting into trouble, or unsure how you will react.

Signs to look out for

- Sudden changes in behaviour, mood, or confidence
- Becoming secretive about online activity
- Reluctance to use devices or, conversely, being unusually anxious about staying online
- Receiving gifts, money, or messages from unknown people

How you can help

- **Keep communication open:** regularly talk with your child about their online life in a calm, non-judgemental way.
- **Reassure them:** let them know it's never their fault if someone behaves inappropriately.
- **Set boundaries together:** agree on privacy settings, who they can interact with, and what information is safe to share.
- **Encourage them to report concerns:** show them how to block and report users on apps and platforms.
- **Act quickly if needed:** save evidence, report the behaviour, and seek support from schools or relevant services.

Key message

Your child's safety online is just as important as offline. By building trust, staying involved, and keeping informed, you can help them recognise risks and feel confident to seek help if something doesn't feel right.

