

Keep your child safe from cyber-flashing

What is it?

Cyber-flashing is a form of online sexual harassment where someone sends an image of their genitals without permission to a device, such as a phone or tablet. It is sometimes called sending 'nudes' or 'dick pics' and is usually done for the person's own sexual pleasure, and/or to cause alarm, distress or humiliation.

Cyber-flashing includes pictures or videos sent:

- Online, such as over a social media platform such as WhatsApp, Instagram or Snapchat
- Through Bluetooth or file-sharing apps like AirDrop that allow people to send images to other devices close by – this is most likely to happen on public transport or in crowded places

People who cyber-flash may go on to commit more serious offences – it's important that incidents are reported so they can be properly investigated.

Under the **Online Safety Act 2023**, cyber-flashing is a criminal offence, and offenders can face up to 2 years in prison. It also requires social media platforms to take steps to prevent cyber-flashing from happening, such as through safety features that recognise and block unsolicited nudes.

4 steps to keep your child safe

1. Tell your child to only add real friends online

Strangers might try and message children online with the intent of cyber-flashing, often by pretending to be a child or teenager. Encourage your child:

- Not to talk to people online that they don't know in real life
- Not to accept 'friend' or message requests online from strangers or anonymous profiles
- Not to make personal information available online for anyone to see

2. Restrict who can send files to your child's phone

Most file-sharing apps allow users to restrict who can send files to them by WiFi or Bluetooth. Find out which apps your child uses, then make sure your child knows how to use these settings.

For AirDrop on iPhones:

- Go to Settings > General > AirDrop
- Select '**Contacts Only**', or '**Receiving Off**' (to not receive AirDrop requests)

Some of the other most popular file-transfer apps include:

- Google Drive
 - Dropbox
 - Microsoft OneDrive
 - AirDroid
-

➤ Zappia

Make sure your child knows to only accept files from people they know.

3. Turn off Bluetooth when not using it

Otherwise, it can be easy for strangers nearby to send images to your child's phone.

To do this on **iPhone**, open 'Control Centre' (swipe down from the upper-right corner or up from the bottom of the screen, depending on the model), then tap the Bluetooth icon (it looks like a '>B'). The icon dims when it's off. Alternatively, you can:

- Go to Settings > Bluetooth > and turn off Bluetooth. It will be grey when Bluetooth is off

On **Android**, swipe down from the top (you might need to do this twice or scroll across). Then tap the Bluetooth '>B' icon to turn it off. It will be grey when Bluetooth is off.

4. Make sure your child knows what to do if it happens to them

If your child doesn't feel in immediate danger, they should report the incident to the police using non-emergency numbers:

- If it happens on public transport, text 61016 or call 0800 40 50 40
- If it happens anywhere else, call 101 or report it online at www.police.uk/pu/contact-us/
- If it happens online, report it on the platform on which it occurred, e.g. Snapchat, so that they can also investigate and ban the account to prevent it happening again

If your child feels scared or is in immediate danger, they should call 999. They should also move to a safe place – and find someone in authority to talk to, such as platform staff, a security guard or a shop manager.

If it happens in school, your child should talk to a trusted adult immediately. If it has happened outside of school, you or your child can still ask the school for support.

Your child doesn't need to collect evidence like screenshots – they just need to tell the police what happened, and to share the details they have, e.g. about the sender, when and where it happened, what was sent. The police may be able to recover the image.

If your child is cyber-flashed by someone they know such as a friend at school, you should report this to the school they attend too. Make sure that they know to never screenshot an explicit image from a person who is under 18, as this is a criminal offence.

It can be difficult for children to tell someone about sexual harassment

If your child tells you about being a victim of an incident of cyber-flashing, make sure you:

- Listen to them carefully
- Reassure them that you'll support them
- Remain non-judgmental

Sources

This factsheet was produced by [The Key Safeguarding](http://thekeysupport.com/safeguarding): <http://thekeysupport.com/safeguarding>

- [Keeping Children Safe in Education, GOV.UK – DfE](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2)
<https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>
- [Online Safety Act 2023, GOV.UK – UK Parliament](https://www.legislation.gov.uk/ukpga/2023/50/enacted)
<https://www.legislation.gov.uk/ukpga/2023/50/enacted>
- [Cyberflashing](#) – Police.UK
- [How to use AirDrop on your iPhone, iPad, or iPod touch, Apple](https://support.apple.com/en-gb/HT204144#setoptions)
<https://support.apple.com/en-gb/HT204144#setoptions>
- [Use Bluetooth and WiFi in Control Centre, Apple](https://support.apple.com/en-us/HT208086)
<https://support.apple.com/en-us/HT208086>
- [Connect through Bluetooth on your Android device, Android Help](https://support.google.com/android/answer/9075925?hl=en-GB)
<https://support.google.com/android/answer/9075925?hl=en-GB>