PARENT FACTSHEET – JANUARY 2020

Keep your child safe from cyber-flashing

What is it?

Cyber-flashing is when a stranger sends an explicit picture, uninvited, to your phone via Wi-Fi or Bluetooth. It's sexual harassment.

It's most likely to happen on public transport or in crowded places.

The file-sharing app AirDrop for iPhone and iPads is most commonly associated with cyber-flashing, but there are lots of different file-sharing apps out there.

With AirDrop, it's easy for anyone to send you images. The automatic preview feature means you also see images without actually opening them.

3 steps to keep your child safe

1. 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 Wi-Fi or Bluetooth. Find out which apps your child uses, then make sure your child knows how to use these settings.

For AirDrop on **iPhones**:

- Open '**Control Centre'** (swipe up from the bottom of the screen or down from the upper-right corner, depending on the model)
- Press firmly on the **network settings card** in the upper-left corner. This will open more connectivity controls
- Tap and hold the **AirDrop** icon
- Select '**Contacts Only'**, or '**Receiving Off'** (to not receive AirDrop requests)

Or, do this by going to Settings > General > AirDrop.

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

- Google Drive
- Dropbox
- Microsoft OneDrive
- AirDroid
- Zapya

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

2. Turn off Bluetooth when not using it

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

© The Key Support Services Ltd | For terms of use, visit thekeysupport.com/terms

Safeguarding Training Centre from The Key

To do this on **iPhone**, open 'Control Centre' (see above), then tap the Bluetooth icon (it looks like a 'B'). The icon dims when it's 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'll be grey when Bluetooth is off.

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

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

- If it happens on public transport, text 61016 or call 0800 40 50 40
- If it happens anywhere else, call 101

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

If it happens in school, your child should talk to a trusted adult immediately.

Sources

This factsheet was produced by Safeguarding Training Centre from The Key.

- How to use AirDrop on your iPhone, iPad, or iPod touch, Apple
  https://support.apple.com/en-gb/HT204144#setoptions
- Use Bluetooth and Wi-Fi in Control Centre, Apple
  https://support.apple.com/en-us/HT208086
- What is cyber-flashing?, Ask the Police
  https://www.askthe.police.uk/content/Q989.htm
- 61016: our non-emergency text number, British Transport Police
  http://www.btp.police.uk/61016_text_service1.aspx

© The Key Support Services Ltd | thekeysupport.com/terms