# E-Safety Awareness

## Parents and Carers

"JUST LIKE IN THE REAL WORLD, WE NEED TO TAKE SENSIBLE PRECAUTIONS ON THE INTERNET TO PROTECT OUR FAMILIES FROM HARM".



#### Age 6 to 9 checklist for online safety

- **Create** a user account for your child on the family computer with appropriate settings and make the most of Parental Controls and tools like Google SafeSearch
- Agree a list of websites they're allowed to visit and the kind of personal information they should not reveal about themselves online (e.g. the name of their school or their home addresses)
- **Decide** time limits for things like using the internet and playing on games consoles. Time limits can be applied on devices such as tablets and laptops
- **Bear** in mind what older siblings might be showing them on the internet, mobiles, games, consoles and other devices, and agree some rules as a whole family
- **Talk** to other parents about their views on things like what age to buy kids a mobile phone.
- Familiarise yourself with age ratings on games, online TV, films and apps, so that you can be sure your child is only accessing age-appropriate content



#### Age 10-12 checklist for online safety

- Make sure you've set some technology boundaries before your child gets their first mobile or games console -it can be more difficult to change the way they use it after
- **Remind** your child to keep phones and other devices well hidden when they're out and about to minimise the risk of theft
- Talk to them about what they post and share online tweets, written comments, photos and videos all form part of their 'digital footprint' that could be seen by anyone and is available on the Web forever
- **Discuss** the kind of things they see online this is the age when they might be looking for information about their changing bodies and exploring relationships, for example
- Hold off letting your son or daughter sign up for services like Facebook and YouTube that have a minimum age limit of 13 - talk to other parents and their school to make sure everyone is on the same page. Be wary that some children 'fake' their date of birth on sites such as Facebook in order to gain access
- **Remind** them that they shouldn't do anything online that they wouldn't do face-to-face



#### Age 13+ checklist for online safety

- **Don't** think it's too late to reinforce boundaries or teach your child anything about technology they might think they have the know-how but they still need your wisdom and guidance
- Talk to them about how they might be exploring issues related to their health, wellbeing and body image online they might come across inaccurate or dangerous information on the Web at a vulnerable time
- **Discuss** how they behave towards others and what they post online. Don't shy away from difficult conversations about things like pornography, bullying and other risky behaviours, such as sexting and inappropriate 'selfies'
- If you give your son or daughter control of their own budget for things like apps and music but make sure you have agreed boundaries so that they manage their money responsibly
- **Discuss** things like downloading and plagiarism so that they understand what's legal and what's not
- Adjust the settings on Parental Controls in line with your son or daughter's age and maturity if they ask you to turn them off completely, think carefully before you do and agree in advance what is acceptable online behaviour



#### Remember

- $\checkmark$  I have asked my child to show me sites they use
- ✓ I have asked my child to only accept people they know and trust in the real world as online "Friends"
- ✓ You can set up safe settings on your computer/laptop and set adult content filters on your child's smart phone
- ✓ My child has agreed to tell me if they are worried about something online





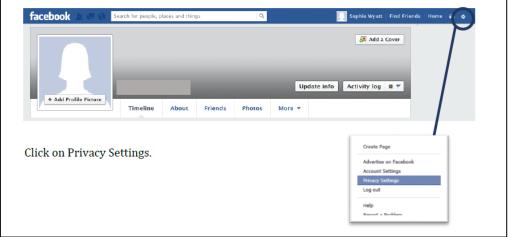
Follow us @NCCcybersafe



Follow these 5 simple steps:

**Step 1:** Ask your child to log into their account as all of the settings in Facebook need to be adjusted within a Facebook profile.

**Step 2:** Set privacy settings. On your child's profile or their Newsfeed, go to the top right hand corner and click on the cog.





**Step 3:** Click on Privacy in the left hand menu. This screen shows you who can see your child's posts and who can find them on Facebook. Click on the links on the right hand side to edit these settings. Anyone registered as under 18 will only be able to share posts with Friends or Friends of Friends.

Privacy	Who can see my stuff?	Who can see your future posts?	Friends	E09
Timeline and Tapping		Review all your posts and things you're tagged in		Use Activity Log
Notifications		Limit the audience for posts you've shared with friends of friends or $Public^{p}$		Limit Past Post
Nobile Followers	Who can contact me?	Who can send you friend requests?	Everyone	EØ
		Where messages do 1 want filtered into my Inbos?	Basic Filturing	E-B
Acos Adverts Payments Support Deshboard	Who can look me ug?	Who can look you up using the email address you provided?	Prends	εú
		Who can look you up using the phone number you provided?	Friends	Edi
		Do you want other search engines to link to your Terreline?	off	EØ

#### Step 4: Take control of the photos and posts your child is tagged in.

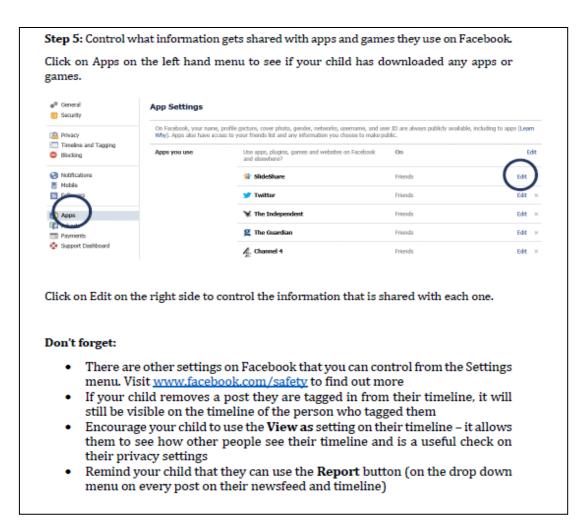
Click on Edit to manage who can post on your child's timeline; who can see their timeline and what happens when they are tagged in a post. Your child can review every post or photo they are tagged in; they can choose Add to Timeline or hide anything they're tagged in.

<ul> <li>Privacy</li> <li>Timeline and Tagging</li> <li>Blacking</li> </ul>	Who can see my stuff?	Who can see your future posts? You can manage the perivacy of things you share by using the audience selector <b>right</b> where you post. This control remembers your selection so future posts will be shared with the same audience unless you change it.			Close
Notifications     Mobile     Followers		What's on your mind?	jk Friends +		
© Apps ₪ Advarts ⊐ Payments Support Dashboard		Review all your posts and things you Limit the authence for posts you/ver of friends or Public?	Public     In Friends     Only me     Octatom		Use Activity Log Limit Past Pasts
-	Who can contact me?	Who can send you friend requests? Whose messages do I want filtered	🔆 Close Friends 🚡 Conneught School For Girls See all lists	1	Edit Edit

6 E-Safety parent and carer

You can manage the privacy of things you share by using the audience selector right where your child posts. This control remembers your selection so future posts will be shared with the same audience unless you or your child changes it.

5 steps to keep you child safe on Facebook







#### Setting your Instagram profile to private

### How do I set my photos and videos to private so that only approved followers can see them?

By default, anyone can view your profile and posts on Instagram. You can make your posts private in the Instagram app so only approved followers can see them. Posts can't be set to private from a desktop computer as Instagram is an app.

To set your posts to private:

iOS

- 1. Go to your profile by tapping 🛄
- 2. Tap Edit Your Profile next to your profile picture
- 3. Turn on the **Posts are Private** setting and then tap **Done**

#### Android

- 1. Go to your profile by tapping 💾
- 2. Tap Edit Your Profile next to your profile picture
- 3. Turn on the Posts Are Private setting and then tap the

check mark to save your changes

#### Windows Phone

- 1. Go to your profile by tapping 💷
- 2. Tap Edit Profile next to your profile picture
- 3. Turn on the **Posts are Private** setting by checking the box and then tap the check mark to save your changes

Things to keep in mind about private posts:

- Private posts you share to social networks may be visible to the public depending on your privacy settings for that network. For example, a post you share to Twitter that was set to private on Instagram may be visible to the people who can see your Twitter posts.
- Once you make your posts private, people will have to send you a follow request if they want to see your posts, your followers list or your following list.
- You'll see requests in your News tab, which you can then approve or ignore. People can send a photo or video directly to you even if they're not following you.

8 E-Safety parent and carer advice booklet

Instagram is automatically set to public so that anyone can see your images - even if you don't know them. It's much easier to stop unwanted contact if your profile is private. When your profile is private, anyone who wants to follow you and see your photos has to send you a request - which you can 'approve' or 'deny'. This way you can control who sees your photos and can make sure only your friends can talk to you on Instagram.

#### **Bullying on Snapchat**



Snapchat can be a really fun way for young people to share images. It's different from other photo sharing apps because when you send an image, it will only last between 1 and 10 seconds before being deleted.

Snapchat can sometimes be used for bullying as well though. This can be really frustrating and upsetting because a young person might get a nasty image which is automatically deleted. This can make it hard to report bullying on Snapchat.

#### How does a young person stop bullying on Snapchat?

They can't save images they get through Snapchat, but if they get an abusive message they can take a screenshot. This way you will have something to report.

If they take a screenshot, Snapchat will try to send a notification to the person who sent you the original message. So it's important to think about how the other person might react if they know they have taken a screenshot of their message.

If someone is bullying your son or daughter over Snapchat, blocking someone will stop them from sending abusive messages. They can also report bullying to Snapchat - they may be able to help stop it.

Sometimes a young person may be added by a username that you don't recognise. This can make it hard to tell whether they know the person or not and it may lead to bullying. It can be upsetting if they are not sure who the person is. A good idea for young people is to set up Snapchat so that they only receive messages from people on their friends list. They can do this by going into their settings then going to 'Who can send me snaps'. From here, change to 'my friends' instead of 'everyone'

#### Five top tips for safe use of social media

It's common knowledge that today's young people are frequent and prolific users of social media. Parents are often worried about the risks of social media use, but there are plenty of safe, sane and responsible ways for young people to interact on these platforms. Below are five top tips from the Parent Zone for encouraging and supporting safe social media use among young people.

**Choose the right privacy settings**. We know that some young people like to set the privacy settings on their social media accounts as low as possible to help them stay plugged in to all the interactions and sharing that goes on. While the impulse to connect with their peers is a good one, there are risks to being too open online and privacy settings can be a valuable tool for safe social media use. Ask your children what privacy settings they have in place already. Encourage them to do things like setting their default sharing option on Facebook to 'friends' (i.e. people they've already connected with) rather than 'everyone'.

Think carefully about photo sharing. It's important to be careful with any information you share online, but photos are especially sensitive. Once a photo is posted to a social media platform like Facebook or Instagram, it can be hard to control whether others view, share or download it. Your child shouldn't share any photos they wouldn't want you, another family member or even a complete stranger to see, and they should be aware that their friends can also upload and tag them in photos. Facebook allows you to review all things you're tagged in using the Activity Log - your child can use this setting to stay on top of what they're associated with.

**If something does go wrong, report it**. Social media sites normally allow users to report violations of their terms and conditions. If your child encounters something inappropriate on social media, they can take action to have it blocked or removed. *CEOP's* Thinkuknow site provides a thorough guide on how to report abuse or inappropriate content, and is an excellent first place to turn if you or your child is worried.

**Get involved**. It's tempting for parents to focus on the risks of social media use, but there are many positive ways for kids to interact online. Lots of people use social media platforms like Twitter and Facebook to stay informed about current events and get involved in activism and advocacy. Young people can also follow artists, scientists, journalists and other public figures to learn more about a range of topics, like music or technology.



**Build friendships**. In addition to getting involved in the broader world, social media can be a great resource for less confident young people who have difficulty with social stress and making friends. Chatting and playing games with friends can seem easier from the comfort of your own home, and these social media interactions may even help some children build confidence in offline social settings.



#### Sexting

#### What is sexting?

When people talk about sexting, they usually refer to sending and receiving:

- naked pictures or 'nudes'
- 'underwear shots'
- sexual or 'dirty pics'
- rude text messages or videos

Images can be sent from a friend, boyfriend, girlfriend or someone a young person has met online. They might have also sent a sexual photo, video or text to someone else.

Before a young person sends a photo, think about:

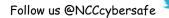
- What could happen to it?
- Who might see it?
- What are the risks? Even if you use an app like Snapchat or webcam - the person can take a screen shot in seconds
- Who are you sending it to?
- Why do you want to send it? If you want to impress somebody, do it in other ways.

Even if images are passed around as a joke there are some serious consequences that may arise.

For further support and information check out the Childline website



Sexting under the age of 18 is against the law as its classed as an indecent image of a child however we need to be providing young people with support and advice around responsible behaviour!



#### Ways to keep it safe

- Explore the games young people are playing. •
- Stick to well known and reputable sites.
- Keep your online identity secure.
- Use strong passwords •
- Limit playing time •
- Age appropriate and follow the PEGI ratings (highlighted below)
- Keep gaming friends in game
- Where do your report concerns? •

#### Risks

- Inappropriate content •
- Large community of "strangers" Young people can be groomed via online gaming •
- Giving away personal information.
- "Griefing" bullying via the online game, deliberately spoiling the game.
- Hidden financial risks •
- Playing the game for too long.
- Warped view of fantasy and reality

Game contains depictions of, or material which may encourage, discrimination



Druas Game refers to or depicts the use of drugs

Fear Game may be frightening or scary for young children



Bad Language

Discrimination

Game contains bad language



Sex Game depicts nudity and/or sexual behaviour or sexual references



Violence Game contains depictions of violence

**Online gameplay** Game can be played online with an age rating and one of the following symbols on the left hand side of the page. Yong people playing games younger than the age rating can have serious consequences. It can leave young people with a very distorted view of the real world compared to the gaming world.

Every video game should now come

#### Online Grooming

Grooming is when someone builds an emotional connection with a child to gain their trust for the purposes of sexual abuse or exploitation. Many children and young people don't understand that they have been groomed, or that what has happened is abuse.

- Vulnerability
- Issues at home are a key marker for online groomers
- Invisibility
- Grooming can take minutes, hours, days, weeks or years
- Language that young people use online anything explicit
- Online naivety
- Suspects will have numerous identities
- Groomers will pretend to be male and female
- Groomers have to be down with the lingo
- Groomers will often bypass filters by asking young people if they are active rather than having sex

If you are concerned about anything suspicious on line you can report it to CEOP

#### Warning Signs - Courtesy of Northamptonshire Police

#### <u>Gifts</u>

- Mobile phones
- Top ups
- Underwear
- Pornography
- Money
- Perfume
- Travel tickets
- I tunes vouchers

#### Person

- Parental reports of change in behaviour, friendships or actions and requests for support.
- Secretive
- Prolonged time on the internet
- Mood swings
- Withdrawn

Remember the vast majority of material on the Internet is legal, decent and honest.



Young people often use text speak over the internet and so do sex offenders below is an example

Some terms	s you may want to know:	
POS	Parent over shoulder	
PIR	Parent in room	
P911	Parent alert	
PAW	Parents are watching	
PAL	Parents are listening	
ASL	Age sex location	
MorF	Male or female	
SorG	Straight or gay	
LMIRL	Let's meet in real life	
KPC	Keep parents clueless	
ADR	Address	
WYCM	Would you like to meet me?	
KFY	Kiss for you	
NALOPKT	Not a lot of people know that	

To name but a few- and they may have changed by the time this comes out!



#### **Action Checklist**

Talk to your child about their Internet use and take an interest. Your involvement is the best way of keeping them safe.

> **Be positive!** The Internet is a fantastic resource for learning, entertainment and communication. Just like in the real world, you need to take a few **sensible precautions**.

Let your child know they can come to you if something they don't like happens online.

Try not to overreact! This could simply make your child secretive about their Internet use and close down lines of communication between you.

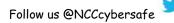
Remember that all the safety advice we have discussed during the session applies to going online with a mobile phone.



If you decide to use software to filter or monitor information from the Internet, talk this over with your child. Any ground rules you agree will be much more effective.

There are three main levels for applying parental controls.

- Internet Service Providers (ISP's). These are the organisations that pipe the internet to your home (like Virgin Media, Talk Talk, Sky and BT). All of the major ISP's provide parental control packages. These can allow you to apply controls across all of the devices that access the internet through your home connection – such as laptops or games consoles.
- Devices that connect to the internet. Most computers, mobiles and games consoles now come with parental controls
  that can be applied. For example, within Windows and the Mac operating systems, there are parental controls that can be
  set for individual devices.
- Software. There are a wide range of packages available to buy or sometimes download for free always look for reputable companies and check out reviews online.



### **E-Safety**

#### Education

All resources can be accessed through the 'Think u know' website.

5-7 year olds

Lee and Kim's Adventures



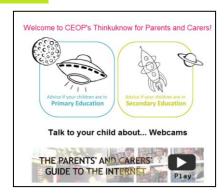
8-10 year olds



#### 11 - 13 year olds

You. Your friends. The Internet.

Keeping yourselves safe, keeping the internet fun.





the information on parental controls in the home

17 E-Safety parent and carer advice booklet



14 +

Sex. **Relationships.** The Internet.

Three things that get a little bit complicated.

Cyber Cafe



#### Further support











