4 ways to keep the kids safe online

The internet can be a wonderful place but the reality is there are dangers for children of any age. Allowing them unfiltered access to the internet you're relinquishing any control you might have over what they're exposed to. Children must learn that they need to behave as well online as they do offline and that bullying is not acceptable – talk to them about it, how to recognise it, and encourage them to report anything inappropriate to you. The NSPCC has a really useful 4-step guide for helping to keep kids safe online TEAM - talk, explore, agree, monitor:

In addition, good general security practices will benefit the kids too:

1. Set up long and complex passwords and multi-factor authentication;
2. Do software or app updates straight away;
3. Consider data... delete old accounts you're not using any more and don't overshare. Use a generic profile picture on accounts, and never the same on multiple accounts to avoid people linking identities.

TALK to your kids and, more importantly, listen to them too. If they're young, discuss with them what they think is nice or bad. Do they understand that grown ups can seem nice but can really be bad? Most importantly, make sure they know to tell a grown up if they see something they don't understand or upsets them, like people doing mean things, let them know to leave the computer open without shutting it down so you can see what they saw and you can take screenshots and report if necessary. With older children, explore why they are vulnerable and why some adults will have an interest in befriending children, and that they might be approached by adults pretending to be children.

It's important children learn that they need to behave as well online as they do offline and that inappropriate behaviour is not acceptable – talk to them about it, how to recognise it, and encourage them to report anything inappropriate to you.

EXPLORE with your kids. Look at what they do online together; that way, you'll get more familiar with it and your young person will be more likely to let you know if anything troubling happens on there. You could even download their app of choice and have a play. Social networks usually have really comprehensive help sites too, full of Q&As. Remember, knowledge is power! As a parent you can't access to your child's account; all users ages 13 and older are considered authorised account holders. Ask if you can regularly review their account together. Explore who they can go to for help, from teachers to you, and reassure them they will never get into trouble even if they've gone along with something for a little while.

AGREE what's ok together. Agree where the kids can they use their devices (is it ok in their bedroom, or at the dinner table?) and for how long? Which sites are out of bounds? More importantly, what are the consequences if they don't stick to the rules? You pay the bill - remind them that means you can see all the sites they visit (even if it is bending the truth slightly!) With older children, discourage them from using their devices in the street as this makes them an easy target and could put their personal safety at risk.

Agree together what your child or young person needs to do if something happens, like they see something unpleasant or get involved in something they shouldn't. You might not be able to promise to do nothing, but you can offer to keep things confidential.

MONITOR what your kids are doing online as much as you can. Speak to your internet provider about filtering - there may be the option to ban specific types of content in your household. Some apps offer kids versions, for example YouTube - this means they can only view child-friendly videos and won't be interrupted by inappropriate advertising, or navigate to inappropriate content. Do also make use of privacy settings in apps (they can be different, see our guides). Check out products like Google Family Link, which allows you to keep an eye on your children and what they're installing; you can even set time limits, or reward them with bonus time, and get to know Google Safe Search which can filter content chosen by you out of searches. Your mobile phone provider can also put caps on spending as another means of monitoring data and monthly usage.

Apps you should know about

Kik: An instant messaging app which only needs an email address to sign up (unlike many others which ask for phone numbers too)

Ask.fm: contains anonymous and unmonitored content.

Whisper: Anonymous social media site.

Monkey: A webcam chat app that connects you to strangers (no longer available from the Apple app store).

SnapChat: Photo sharing app, but location tracking is active unless switched off and photos 'disappear' after a short time.

Omegle: App to connect with strangers. See also **ChatRoulette**.

YikYak: allows users to create and view networks based on proximity/location.

Habbo Hotel: Social networking community aimed at teens.

Search Get Safe Online and Net aware for more on these:

https://www.getsafeonline.org/personal/article-category/safeguarding-children/

https://www.net-aware.org.uk/

Snapchat

68% of 12 to 15-year-olds have a Snapchat account. The app lets you send photos, short videos or messages to friends. Pictures and videos, known as snaps, usually appear temporarily before disappearing, though they can be captured via screenshot or replayed once more.

Snapchat features to be aware of:

- It can share your real-time location if you don't use 'ghost mode';
- People can screen shot images you share so they might not disappear;
- You can get requests from people you don't know - accepting the request (known as "adding them back") will reveal any messages.
- You can make a 'private story' where you can customise who sees it.

Keep it to friends only - everything shared is publicly available unless you change it
Make sure your child knows that to change the settings, they need to hover over 'View My Story'. You can then modify the settings to suit your preferences - the 'My Friends' option allows only your friends on Snapchat to view your profile. If you want only selected users finding out about you, use the 'Custom' option. To avoid receiving snaps from strangers, click the gear button on the left square button of an open Snapchat. That should lead you to the prompt 'Receive Snaps From' - choose 'My Friends'. Also, make sure your child knows to check any 'friend' requests are from people they know before accepting them.

Turn on 'ghost-mode'
When ghost-mode is enabled, the user's location will remain private. To turn in on, open Snapchat, tap the circle or your icon in the top left-hand corner of the screen. Next, tap the 'Settings' icon located in the top-right hand corner. Tap the toggle feature so it's blue. If it's disabled (grey), you can choose from three other options – 'My Friends, 'My Friends, Except' and 'Only These Friends' allowing your to select specific friends. Our advice is for your child not to be sharing their location at all. Snapchat launched a new feature called 'Explore Activity' earlier this year which lets users search for content by location – one to be aware of.

Turn on two-factor
This is an easy way to help strengthen security on the account. Go to 'Settings' then 'Two-factor Authentication'. This means your child will get verified via a text message whenever they're logging in.

Your Snapcode
A Snapcode is a scannable code that makes adding new friends even easier. Any user can automatically become a friend on Snapchat by scanning your Snapchat QR code. It's best to avoid publishing your Snapcode or username on social network platforms to avoid being inundated with new friend requests.

Block accounts you don't know
Talk to your child about the importance of blocking any user who shows any inappropriate behaviour, or if they're being approached by strangers. It's really easy to do; block a user by clicking on the person and pressing 'Block'. To block someone from your chat history, tap 'Chat' in the

bottom left-hand corner. Choose who you want to block by tapping and holding down on their name. Tap 'More'. Next, tap 'Block', confirm you want to block by tapping 'Block' again.

Know how to report
To report someone to Snapchat, tap 'Chat' in the bottom left-hand corner. Choose who you want to report by tapping and holding down on their name. Tap 'More' > 'Report', then select the reason you want to report them and follow the prompts. It might be they're posting inappropriate content, are impersonating someone, or they're a spam account. Whatever the reason, be sure to report. This will help to protect others. To report something else (not a person), scroll down to 'Support' and tap 'I Need Help', then tap 'Safety' and choose what you want to report. Follow the instructions shown on screen.

TikTok

TikTok is the video app to be on if you're generation Z. It is the world's fastest-growing social media platform - it has an estimated 689 million monthly users (mostly aged 16-25) worldwide, and the app has had more than 2 billion downloads on the App Store and Google Play. It was only launched in 2017, but it feels longer and if you haven't yet recorded a TikTok dance routine, then where have you been?

The usual social media risks apply - use privacy settings to limit how much your child can share and talk to them about the risks. To help maintain some privacy, sign up to TikTok separately and not by using Facebook. This stops people being able to link the two accounts and learn more than they should.

Keep it private
Set the account to private which will only allow friends to contact them using the app or see any videos they upload. It restricts some of the freedom of the app but is a useful protection.
1. Open the TikTok app and select Settings.
2. Select Privacy & Safety from the menu.
3. Toggle Private Account to on.

You also have the option to control who can post comments, who can show reactions, who can duet and who can send messages. Setting these to 'friends' limits those who can interact with your child's content.

Restricted mode
This limits content that may not be appropriate for teenagers and is activated using a password, which will be valid only for 30 days. Go to the TikTok app and tap the profile icon in the bottom-right corner > Tap the three dots menu in the top-right corner > Tap 'Digital Wellbeing' under the 'General' tab > Tap 'Enable Restricted Mode' on your screen > Set a 4-digit passcode and tap the Red arrow icon > Enter and confirm the passcode once again.

Set screen time limits
Set a limit, after agreeing one with your child, to help manage time on the app. If you exceed your screen-time, TikTok will prompt you to enter a password before you can continue using the app. To set a limit, go to the TikTok app and tap the profile icon in the bottom-right corner > tap the three dots menu in the top-right corner > tap 'Digital Wellbeing' under the 'General' tab
Step 4: Now, tap 'Screen Time Management' on your screen (by default, the time limit will be set to 60 minutes; you can customise the time limit here > tap 'Enable Screen Time Management'.

Filter comments
TikTok also allows users to manage comments by filtering out words they deem undesirable. Each user can choose up to 30 keywords in Hindi and English. **To filter comments, g**o to the TikTok app and tap the profile icon in the bottom-right corner > tap the three dots menu in the top-right corner > tap 'Privacy and Safety' and then tap 'Filter Comments' > tap the switch at the top of the screen and tap 'Add Keywords' > add up to 30 keywords you want to filter.

Instagram

If it's not Snapchat, it's Instagram, or so the figures show. 66% of children aged 12-15 have an profile on the popular photo-sharing app - just slightly behind figures reported for Facebook and Snapchat as of the report in 2019. Instagram is a photo-led social media platform (it was actually purchased by Facebook in 2012). While it may have a different feel to it, it's no different to any other in that the usual social media risks apply - diligent monitoring, filtering, and regular communication with your kids will help to keep it fun and safe. Here are our top tips for making sure your kids stay safe and enjoy connecting with their friends, and the outside world:

Make your account private
Use privacy settings to limit how much your child can share, and talk to them about the risks; there may be people on the platform who don't know your child but will request they follow them, or try and persuade your child to reveal more than they should. Teaching children to recognise any attempts like this and report them to you is key. By default, accounts are public when you set one up. Make sure you child's account is 'private' so they can only connect with friends and people they know. To make an account private, go to the profile, tap Settings > Privacy > Account Privacy and tap next to 'Private Account' to make the account private. Once the account is set to private, users will have to send you a request to follow you, which you can either allow or deny.

Don't share locations
Make sure Photo Map (geo tagging) is off on photos. If your child has activated their Photo Map they can remove all map-approved photos, which will disable their Photo Map. Navigate to profile, tap the 'Photo Map' button that appears in the upper right corner, navigating to the stacks of images that appear, and deselect all images (tap green check marks) in the grid review view.

Exploring Insta
The news feed makes it easier to discover photos posted by others whom you follow on Instagram. The 'Following' tab on your news feed shows activity among those you follow. It will display photos they have liked, other users they've started following, and comments between users that you are following.

Blocking users
The only way to remove someone from your list of followers is to block them. To **block a user,** navigate to their profile page, tap the button in the top right corner of the screen (arrow in box icon), and tap "Block user" to prevent the user from viewing your account.

Know how to report
Report a user with Instagram's built-in flagging feature. In order to flag a photo tap the "…" (three dots icon) below the photo you want to report and then choose "Report Inappropriate." Photos can be reported for nudity, prohibited or illegal content, violence and gore, or the promotion and glorification of self-harm.