Keeping Safe Online

A Guide for Parent and Carers. Created with Children and Young People in Barnsley.

4.27



Teleg











MAY 2024







Background image: Asset from Freepik.com

Introduction

Contents

Pages 04-10: Popular Apps

Pages 11-15: Privacy Settings, Inappropriate messages & Reporting

Pages 15-16: Online Bullying

Pages 16-17: Hate Crime and Extreme views

Pages 17-18: General advice This guide has been created with help from children and young people across the borough, who told us the apps that they most commonly use, the issues that they encounter, and how they stay safe while using them.

On the following pages, you will find details about specific apps that children and young people use, settings that you can enable to stay safe online, and where to go for help if you have concerns or worries.

Remember

You can always get advice from schools and colleges – ask to speak to your Designated Safeguarding Lead (DSL), Head of Year / Student Support Officer or Form Tutor.

These are the most popular apps used by our children and young people in Barnsley



TikTok Age restriction = 13+



Instagram Age restriction = 13+

£

Snapchat Age restriction = 13+ **Purpose:** Share, create & watch short videos. Gain 'followers' who like, comment, and view your posts. For users registered as 16+, their profile is 'public' by default and their videos can be viewed and downloaded by anyone.

Duetting & stitching: Creating a video to post alongside someone else's or taking parts of other people's videos and reposting them with your own.

Private Messaging: Users aged 16+ can send private messages to one another. These can be from anyone online.

Downloading: Unless it is turned off in settings, people can download a copy of your videos to their device to keep forever.

Purpose: Share content (videos & pictures) that followers can interact with by viewing, liking, and commenting. Instagram may push a narrative of a 'perfect world', and users may feel pressured to post perfect, polished images of themselves.

Location sharing: Users can tag their location on their profile posts and in stories which can then be viewed by followers. This could leave young people open to risks, such as strangers gaining access to their location.

'Supervision': A parental control offered by Instagram. Parents create their own Insta account and then link it, but the young person needs to accept an 'invitation link' for this to work – it is their decision. Parents can then set break reminders and view followers, but not read private messages or block accounts.

Purpose: A popular image sharing and messaging app that lets users exchange pictures and videos (snaps), with photo effects and filters, which then disappear. The 'disappearing snap' feature of Snapchat can lure young people into a false sense of security, and they may send images that they would not usually send.

Snap Map: A feature that shows the real time location of all users on an interactive map. This feature is 'on' by default. You will need to activate 'Ghost Mode' to stop your location from appearing on the map - Click on your profile icon, then scroll to snap map. Click on it, then the cog in the top right corner to enable ghost mode.

Disappearing messages: People think that because messages and pictures disappear, they are gone forever. Users can screenshot content and share it: if they take a picture of their phone with another device, you will never even know. If someone is sending inappropriate content over Snapchat, it can be much harder to prove - report their content immediately by pressing the message or snap. To report or block someone, press, and hold on their Snapchat ID, and select 'Manage Friendship'.



WhatsApp Age restriction = 13+



Facebook Age restriction = 13+

Purpose: Users can send text, voice, and video messages, make voice, video calls, and share information and documents. Only people who have an account can send and receive messages, but depending on privacy settings, anyone can contact you or add you to group chats. By default, WhatsApp automatically sets privacy settings to public – these need to be changed in your settings.

End-to-end encryption: A form of message security; It means that only the sender and recipient can read what is sent – moderators (including WhatsApp themselves) and third parties cannot view any of the content. While this offers more security for those over 18, this could lead to online safety risks for children and teens.

Groups and Communities: Groups are normal chats that include multiple users. Anyone can add a user to a group unless their group privacy settings are changed within the app. 'Communities' works like online forums. A community might contain multiple groups that people can join and chat to others in. These chats are end-to-end encrypted as well.

Location tracking (Live Location): Automatically turned off on WhatsApp. When turned on, users can see your live location – keep this off in settings to minimise risk.

Purpose: A social media platform for sharing images, text & videos. Users can add other people as 'friends' in an online network and share updates about themselves. Users can like, react, or comment on statuses, images, videos, comments & much more on the platform. **News:** Facebook also encompasses businesses, organisations & news, making it a huge source of digital information sharing. Remember that not everything that you read on Facebook is necessarily true, and sometimes people can share material that is offensive – be sure to report any content like this.

Marketplace: People can advertise and sell goods / services in their local areas. The safest way to use the marketplace is by asking an adult to message the seller on your behalf. Watch out for scams, no matter how genuine someone may seem, and never go to collect an item from someone without an adult present.



Messenger Age restriction = 13+ **Purpose:** An instant messaging app linked to Facebook, popular for group chats, sharing images and videos. This app is also popular for playing games with friends. It can allow young people to connect with strangers, receive message requests from strangers and video call. **'Secret conversations'**: Messages timed to disappear can be sent to others, similar to Snapchat. They may be used to send bullying or sexual messages.

'Message requests': Users who are not friends on Facebook can still message other Messenger users through this folder. This could open opportunities for scams or bullying. Ensure only Facebook friends can stay connected by switching off the message requests section, which is 'on' by default.



YouTube Age restriction = 13+ without parent or guardian. Any age with parental consent / set-up

Purpose: A popular video sharing and social media platform. Videos can be commented on, liked, and shared.

YouTube Kids: A separate app made for children under 13. This app offers controls to restrict search and content, set time limits, and manage watch history to help promote internet safety. Parents can also set a passcode to ensure only they can change settings in the app. Supervised Accounts: Parents who decide that their child under 13 is ready to explore the main YouTube site can set up a supervised account, linked to a parent's own Google Account. When a parent sets up a supervised account, they select a content setting that limits the videos and music that children under 13 can play. Subscribing to Channels: Subscribe to channels that you feel comfortable with. This creates a feed of safe videos to browse and watch in the 'Subscriptions' area of YouTube.



X / Twitter Age restriction = 13+

Purpose: X is the new name for Twitter - an online 'micro-blogging' social network. It is known for its short character limit of 280 characters and its use of hashtags, threads, and trending topics.
Location reveal: Tweets can be geotagged, which could broadcast a user's exact location (or favourite places to hang out) to others.
Privacy: All Tweets are public by default, meaning anyone can view, reply, and retweet regardless of their age or beliefs.
Adult use: A higher ratio of adults on the platform means age-inappropriate content is more likely to be viewed by younger users.



Roblox Age restriction = 7+



Discord Age restriction = 13+

Purpose: An online gaming and game creation platform. Users can play and create games for others to play. It also includes social features such as friend requests and chats where players can design an avatar and speak to others while they play.

Risks: Roblox has previously faced criticism following harmful sexualised content being prevalent on the platform.

Parental Controls: Safety settings are enabled by default for children under 13 - which is why registering with a real date of birth is important. Most games have a public server, which means that users can interact with strangers if safety settings are not in place.

Purpose: an instant messaging social platform, in which people enter 'servers' so they are part of a group – commonly used for gaming communities. Some servers are NSFW (Not safe for work – often meaning inappropriate/ adult content) and may have content age-inappropriate for younger users.

Servers: All users can create their own server for free. Servers are based on individual topics or interests (such as Among Us, reading, or sports teams). They can be public (anyone can request to join) or private (requires an invitation from admin/moderators). Once granted access to a server, users can participate in an open chat with other users from all over the world. Many young people use the 'screenshare' option to communicate with each other while watching films, playing multiplayer video games, or watching sport matches. There are private chat options available as well.

Privacy: User accounts also cannot be made explicitly private. The privacy setting 'Keep Me Safe' can be enabled – it scans all direct messages to block explicit content and restricts access to NSFW servers.



Telegram Age restriction = '17+' on the Apple App Store. Google Play advises 'Parental Guidance'

Purpose: Telegram is a cross-platform messaging app that combines familiar elements from platforms like WhatsApp and Twitter into one app; It allows users to communicate with individuals, small groups, or large groups (up to 200,000 people). The ability to connect with others in the area may lead to young people disclosing locations and personal details that could lead to grooming or harassment in-person. **Risks:** Telegram features unmodified chats with lots of inappropriate content, especially through the 'groups / people nearby' feature. Parental supervision is **strongly** advised.

Secret Chats: Also known as 'disappearing messages', users can set 'self-destruct' times on messages, ranging from 2 seconds to a week.

Channels: A tool that lets a group of administrators or an individual administrator broadcast messages to an unlimited subscriber base. Channels can be used by groups with radical views to spread hate.



Reddit Age restriction = 13+

Purpose: A social news website and forum where users can upload, share, and promote content. It's made up of thousands of different communities that users can subscribe to, on topics ranging from niche to popular hobbies, memes, and media.

Subreddits: A subreddit (or sub) is a community based on a particular topic or purpose. Users subscribe to subs that interest them and can either browse individual subs or visit their home page. Users post content on subreddits, then other users interact with these posts by commenting, upvoting and sharing.

Controversial Subs: The site has faced criticism for hosting hate group communities, sexual and graphic content. Reddit may create communities that reinforce dangerous or unhealthy beliefs, with some communities being accused of encouraging incel behaviour, racism, and other extremism.

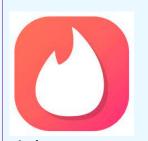
Anonymity: Users can remain anonymous, with only a unique username differentiating their profile from anyone else's. This means young people could be targeted by predators. Users masking their identity is a concern when young people might be tricked into believing they are talking to 'friends' or other teenagers.



Twitch

Age restriction = 13+ (under 18s must have parental consent via agreeing to terms & conditions) Purpose: A live streaming video platform which allows creators to broadcast and users to watch content, usually about games, including eSports. Twitch streams are often live and are therefore difficult to moderate. There are few limits on what can be shared on Twitch, which in turn poses significant safeguarding risks. Twitch came under scrutiny when popular streamers broadcast inappropriate and sexual content. Gifting and Spending: Twitch users can follow other people's channels for free or subscribe for a fee. Users can interact with the live streamer through a chat feature and can even donate in-platform currency called 'bits' to support them. There are also exclusive streamer features available for users with a paid monthly subscription. Young people might feel pressured or encouraged to spend money on streamers. Risks: Parents and carers cannot enable safety measures or monitor content. Once an account has been made, the user is able to livestream immediately, so children may livestream themselves to strangers without thinking of the consequences.

Privacy Settings: All profiles are public and cannot be made private. Anyone can access and watch livestreams without registering.



Tinder Age restriction = 18+ **Purpose:** An adult–only dating app. When asked, some young people in Barnsley said that they had used Tinder.

If you are under 18, we recommend that you delete this app. Risks: Underage users may receive inappropriate messages, photos, and videos. Dating platforms attract scammers – people who use romantic relationships to extort others, typically through lying or blackmail. Some of these can be very elaborate and rely on emotional manipulation. A young person may not have the emotional capacity, knowledge, or confidence to identify a scam and if they are caught in one, they may feel shame, panic, and stress.



BeReal. Age restriction = 13+ **Purpose:** A once-a-day photo sharing app – users are given a 2-minute window to share a photo of themselves and their surroundings to their friends. BeReal asks users to take a quick snapshot of an 'authentic moment' during their day to share with their followers. There are no filters or opportunities to stage the 'perfect photo' – what you see is what you get. It is formatted to make the user show their 'real self'. **Risks:** If young people accept contacts they do not know, it is easy to build up a picture of routines in daily life, for example, school uniforms, bus stops and regular locations. The format of the app leads to addiction issues, with users prioritising it because of the time limits it sets. Safety settings are lacking – there are no privacy features, no parental controls, and no blocking abilities on this platform: just reporting. A 'discovery' page encourages interaction between complete strangers and could lead to communication on other apps with messaging functions (like Instagram or WhatsApp).



Wattpad Age restriction: 13+ **Purpose:** A social storytelling platform where users connect with their favourite writers, read, and write original stories. Wattpad has a variety of features to categorise their stories and distinct types of content, which can help users avoid inappropriate content or find the exact kind of topic they want to read and write in.

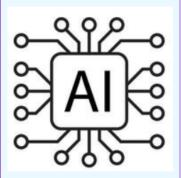
Story Tags: Wattpad hosts diverse types of content and some of it is adult in nature. Because any user can add a story, it is up to them to add the appropriate tags. If a user comes across a story that is not accurately labelled, they should report it. Users can also filter mature content out of their recommended stories.



Pinterest Age restriction: 13+ **Purpose:** An online image-sharing platform. While Pinterest is not the top app among young people, some teenagers in Barnsley do still engage with it. Users can browse thousands of posts called Pins to get ideas for recipes, decor, teaching and more.

Risks: Some posts may spread misinformation. Interacting with it results in more of the same, which leads to close-minded thinking or inaccurate ideas about the world. Users might come across inappropriate content for their age; while Pinterest's content guidelines clearly prohibit inappropriate content, reports show it sometimes slips through the filters.

Purpose:



Artificial Intelligence (AI)

Artificial intelligence (AI) makes it possible for machines to learn from experience, adjust to new inputs and perform human-like tasks. Most AI examples that you hear about today – from chess-playing computers to self-driving cars – rely heavily on deep learning and natural language processing.

Al can:

- Enhance learning experiences such as assisted-learning across diverse topics including science, tech, poetry, music and arts
- Provide instant answers to burning questions
- Engage children in fun conversations
- Improve critical thinking skills

Risks:

- Cyberbullying and sexual harassment: The use of AI-generated text or images to bully or sexually harass children/young people.
- Generative child sexual abuse material (CSAM): Al tools that allow perpetrators to generate CSAM material offline, where detection is not possible; and Al tools that can be used to generate CSAM images from images of real children (e.g., famous children, or children known to perpetrators).
- **Disinformation and fraud:** The use of plausible-seeming Algenerated text in the service of disinformation or fraud.
- Impacts on education: The use of AI tools that may undermine formal assessments and, ultimately, negatively impact on children's learning.
- Privacy concerns: AI tools rely on large datasets and there are important implications for how children's data is used and their privacy protected.
- **Bias or discrimination:** Bias in the design of systems or their underlying data leading to discrimination against some groups.

Privacy Settings, Inappropriate Messages & Reporting

In the UK, it is a criminal offence to make, distribute, possess or show any indecent images of anyone aged under 18, even if the content was created with the consent of that young person.

Privacy Settings and how to use them

Follow these tips to help your child explore the internet safely. If you have an older child who creates their own accounts, use this information to talk to them about how they can use privacy settings.

1. Check the audience.

Before your child shares content online, check who will be able to see what they post. You need to make sure that personal information can only be seen by small groups of friends who they know and trust.

Most apps allow you to change who can see your posts, who can contact you and who can look you up. You can even control who can see different parts of the content you share. For example, apps like Snapchat, Instagram and Facebook allow you to share 'stories' with smaller audiences, rather than your entire friends list.

2. Switch off location sharing.

It is become increasingly common for apps to allow users to share their location. Many social media and live streaming platforms make it easy for you to broadcast what you are up to and where you are.

Some apps like Facebook and Instagram allow you to tag your photos with the place they were taken. These tags can list the exact address of your location, not just the city or general area they were taken in.

Other apps track users' locations and update them automatically. For example, Snapchat's 'Snap Map' location sharing feature can update your location whenever you have the app open. Its default setting is 'Ghost Mode' which prevents friends from seeing your location. However, some young people turn it on to let their friends see their whereabouts.

Remind your child that sharing their location online is risky. It could put them at risk of unwanted contact from strangers. Find out how to turn your child's location sharing services off, or make sure that they are only sharing it with people they know and trust.

3. Check the tagging settings.

It can be difficult to control information that others post about you online. Unless the content is abusive and violates community guidelines, it will not be taken down by the platform. However, privacy settings can be used prevent private photos or information about your child from appearing on their profile.

4. Review all privacy settings regularly.

Many websites and apps periodically make changes to the privacy and security settings that they offer. Frequently review your child's privacy settings to ensure they are unlikely to encounter the risks associated with sharing personal information widely.

Some sites or apps like Facebook allow you to view how your profile looks to the public (people you are not friends with). Use this tool to check that you and your child are happy with the information they share to people they don't know.

Adults should regularly review their privacy settings too. If you posting pictures of your child/young person, you may wish to think about how this could affect their online footprint for years to come.

When your child/young person downloads a new app, always check your settings, and read their advice on how to report and block. This is especially important in apps such as Snapchat, where the messages disappear after a certain time limit.

Age Rating = 13+

If your child is aged **13** – **15** years old, many apps (such as TikTok and Instagram) will automatically sort out your privacy settings for you. But, if your young person is **16 or over** – *or their account thinks that they are* - they will need to adjust their settings manually to stay safe.

Our research tells us that many children in Barnsley, including primary age children, lie about their age to get access to apps such as TikTok: If you find that this is the case, talk calmly to your child/young person about the risks involved and take action to keep them safe.

Direct Messages

DM usually stands for Direct Message. This is a private mode of communication between social media users. When you send a direct message, only you and the

recipient can see the content. Instagram, Facebook and X (formerly Twitter) all have direct messaging platforms.

If your child/young person is under 16, private messaging is automatically turned off on some apps, such as TikTok, but even then, we recommend that your child/young person keeps this feature off: it can be really dangerous to have a public account where people can message you whatever content they want.

Direct messaging leaves your child/young person at risk of hurtful or offensive comments 24/7, with no escape, so be sure your child/young person blocks anyone who makes them feel uncomfortable.

'Finstas'

Finsta is short for Finstagram, or "fake Instagram," referring to an account made so that a user can post images and interact with other accounts in a more private way, usually reserving the account's followers

to close friends. It can be on any platform, including TikTok and Facebook, but Instagram seems to be the most popular. These types of accounts use Fake names to avoid using real names

Anonymity and lack of supervision might encourage children/young people to engage in unlikely behaviour, such as posting sexually explicit content, pursuing dangerous political ideals, or bullying. Others with access to the account may take screenshots of posts and send them to others, or reveal the identity of the account owner.

Finstas are an easy breeding ground for cyberbullying. When users see a request from a Finsta, there's often no information to identify the account's real owner. The secrecy of Finstas give bullies the perfect chance to troll kids without consequences. Finstas are also hard to find, which means it's hard for parents/cares to check or control this type of account. These factors leave a space for potential bullying and hateful posts.

Some Finstas serve as a space to post funny and embarrassing photos teens would never show on their real Instagram. This light-heartedness can make a serious Finsta post seem like a joke.

Everything you post on the internet is there forever. But, for digital natives, that idea can be hard to grasp. In a lot of cases, Finstas hold explicit content. Teens use the account's anonymity to hide from parents/cares and school. Yet, once out there on the internet, it's there forever.

A risk of posting content online is that people will end up with permanent access to it: anything that your child/young person put online has the potential to be online forever.

They might not be thinking about it now, but in future, things that they post may come back to haunt them; many influencers have been caught out by content they posted when they were younger. Things that they post privately may end up being leaked to family, friends, and even their schoolteachers, so think really carefully about what you post. Even with a private account, anyone can see your profile info on most apps, so don't share your full name or where you go to school.

Sending of Inappropriate / Indecent Images or Messages

The Government has released Guidance for Parents/Carers in March 2024, regarding Inappropriate and Indecent images.

Parents/carers whose child has had their nudes or semi-nudes shared publicly should be advised to:

- Stay calm and refrain from getting angry with their child.
- Help their child delete images from social media accounts (included from cloud photo backups) if they have uploaded them themselves.
- Support their child use the IWF and Childline's Report Remove tool to report an image that
 has been shared online: www.childline.org.uk/info-advice/bullying-abuse-safety/onlinemobile-safety/sexting/report-nude-image-online/. They can also help their child to use
 NCMEC's Take It Down tool to help them remove or limit the spread of nudes or semi-nudes
 that have been shared online: https://takeitdown.ncmec.org.
- Report sexual images on individual sites to get them taken down. If the image has been shared via a mobile, they should be informed that they can contact the mobile phone operator to have a mobile number changed.
- Go to services for Harmful Sexual Behaviour, such as the National Clinical Assessment and Treatment Service (an NSPCC service) or Shore (a Lucy Faithfull Foundation service, if there have been similar incidents or they are worried about inappropriate sexual behaviour for their age.
- Speak to their child's education setting if they are concerned about any bullying behaviour.

Parents/carers whose child has been sent nudes and semi-nudes should be advised to:

- Listen to their child's concerns without criticising their decisions.
- Consider ways that their child could speak to the sender to stop future correspondence. Alternatively, if the child or young person prefers, show them how to block the sender.
- Discuss issues of consent and trust within healthy relationships. Explain that it is not ok for someone to make them feel uncomfortable, to pressure them into doing things that they do not want to do, or to show them things that they are unhappy about. Children can speak to school and/or parents/carers if this ever happens.

Parents/ carers whose child has shared another child's nudes or semi-nudes should be advised to:

- Stay calm and refrain from getting angry with their child.
- Discuss issues of consent and trust in healthy relationships or friendships. Talk about the types of things which are and aren't ok to share and how they would feel if someone shared a personal photo of them.
- Contact their child's education setting if they are concerned that their child is behaving in a sexually inappropriate way. They could also be directed to services for Harmful Sexual Behaviour, such as the National Clinical Assessment and Treatment Service, if appropriate, or if similar incidents have previously occurred.

Online/Cyberbullying Bullying

Online bullying, or cyberbullying, is when someone uses the internet to target and deliberately upset someone.

Cyberbullying often happens on personal devices that young people have continuous access to. This means it can happen anywhere and at any time, so it can feel like it's hard to escape. The bully could be either someone that they know, or a complete stranger.

It can be hard to control the spread of messages, images and videos sent online, which means many people could see them in a short period of time. However, online bullying can leave a trail of evidence which can be helpful when dealing with the incident and reporting it.

Encourage your child to save the evidence and show you

They can do this by taking a screenshot of what has happened or by keeping the messages they have received.

Don't deny access to technology

Although it can be very tempting to remove a device from a child if they are being bullied online, it may prevent your child from coming to you about online worries again.

Don't reply

Most of the time a bully is looking for a reaction when they are being mean online. Tell your child/young person not to reply. Instead, they should tell a trusted adult what has happened.

Use the tools available

Report, block and take a screenshot. You can report a person or profile, as well as content, e.g. a post, video or comment. This will then be flagged to the service who will review it against their terms and conditions.

Speak to the school

It is always worth having a conversation with your child/young person school about their experience of cyberbullying. Schools can offer support and advice to you and your child. Consider contacting their class teacher, form tutor, Head of Year, or a pastoral lead.

Group Chats, Extreme Views & Being Asked to Download Content

With social media being such a big part of children/young peoples' lives, it can be easy to make friends online who they have never met in 'real life'. They might be someone in a group chat that they have been added to, someone with similar interests to them that they have met on a forum, or someone who they game with online.

At the start, they might think that they have a lot in common – otherwise they would not be speaking to them in the first place. They might be keen to be their friend, and they might think they understand them more than other people that they know.

But then, they realise that they have strong views on certain topics, such as:

- Women / girls, sexism, or 'incel' type behaviour

- Immigration and race – this might be disguised as being overly 'proud' to be white and British, to the point that they dislike other races or types of people in society

- Transgender / non-binary issues or LGBTQIA+

- They might not be very noticeable at first, such as tagging them in a meme or a 'joke' about such things to see how they react.
- They might not want to disagree with them, because they feel that they are their friend.
- They might not want to disagree with them in a group chat, as other people might share the same views.
- They might hold status in the game that they play, and they are worried that they will get kicked out of the group if they speak up.

People might ask your child/young person to download links, follow links or share material. Sometimes, this material may be illegal for them to distribute or even possess, so they should never share it.
If anything like this happens to your child/young person on an app, group chat, or on their team in a game, ask them to leave the server, group or team, report and block.

If you are worried about online sexual abuse or the way that someone has been communicating online, let CEOP know at:

https://www.ceop.police.uk/Safety-Centre/



What kind of things do people report to CEOP?

Some of the things reported include:

- Someone online has been asked to send nude images
- Sharing a nude image with someone online and then being threatened
- Doing something embarrassing on a webcam, and the person then turning nasty
- Live-streaming and doing inappropriate things
- Asking to meet face-to-face and feeling pressured
- Online talking about sex, and feeling uncomfortable
- Putting on pressure to do things
- Online gamers trying to talk privately

Links to further support and advice

Concern	Contact
Online Bullying	https://www.nationalbullyinghelpline.co.uk/
Parent/Carer Advice line	<u>https://www.kidscape.org.uk/advice/advice-</u> for-young-people/
Homophobic, biphobia and/or transphobic bullying.	<u>https://each.education/homophobic-</u> transphobic-helpline
Radicalisation/Extreme views	https://www.educateagainsthate.com/parents/
Gambling or spending money online	https://bigdeal.org.uk/
Child Line: Help with any problems	https://childline.org.uk
The Mix	https://www.themix.org.uk/
Mental Health ~ Shout	https://giveusashout.org/
Mental Health in Barnsley ~ Kooth	https://www.kooth.com/

Background image: Asset from Freepik.com

