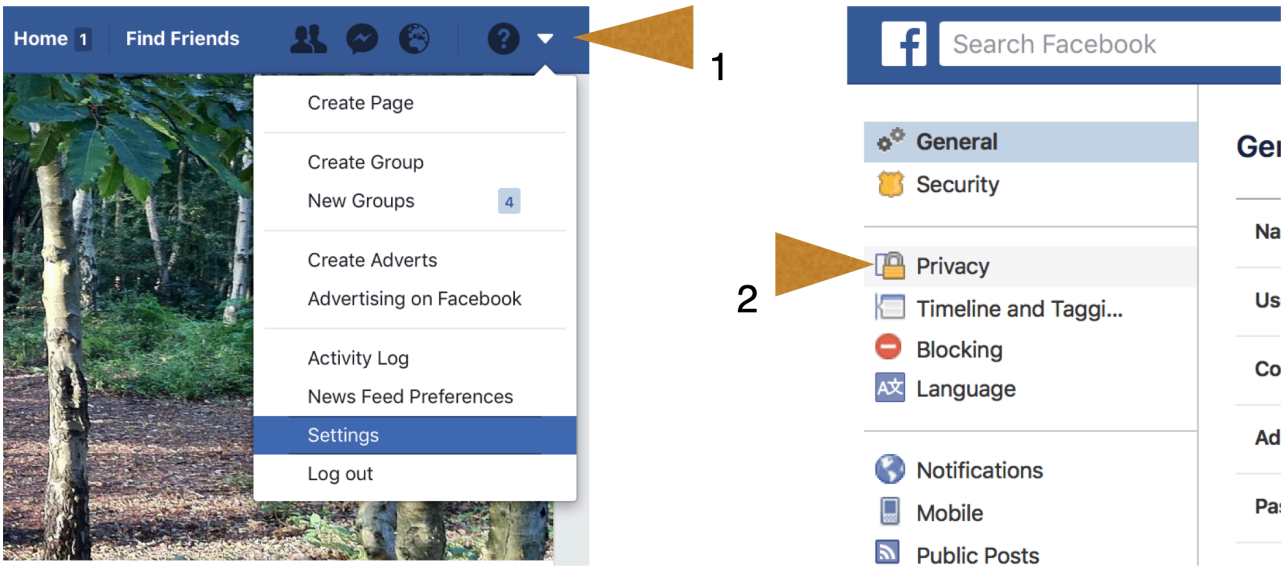
eSafety for Parents

Facebook - How to set up your account for Privacy

Nearly all Social Media platforms have privacy settings, allowing users to decide how much information to share. Facebook is one of the most common. To change privacy settings in Facebook, log in using a web browser, then clicking the question mark (1) in the top-right corner. Next, choose 'Privacy' (2) and then change all the settings below it to 'Friends only'.



Privacy Settings and Tools

Your activity	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
How people can find and contact you	Who can send you friend requests?	Everyone	Edit
	Who can see your friends list?	Friends	Edit
	Who can look you up using the email address you provided?	Friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit
	Do you want search engines outside of Facebook to link to your Profile?	No	Edit

Other Social Media networks

younow
Go Live

YouNow (13+). A live streaming service in which users can view others' video streams, or stream themselves singing, driving, posing, etc. Viewers can comment on feeds live, and 'tip' broadcasters. Comments and content can be suggestive and unpleasant. Users can buy 'bars' to tip broadcasters, who get real money. There has been an issue reported in Durham in which children were encouraged to expose themselves on feeds using the #TruthOrDare hashtag.

TikTok (13+). Users record videos of themselves miming to music, dancing or performing. Videos are shared with a potentially global audience; users can comment on others' work. Negative comments are common; 'trolling'. As a consumer, there is the risk of being exposed to content of a sexual nature.

Tinder (18+). A dating app for adults; users flip through photos of other users, swiping the screen to decide who they like. Mutual 'likes' can message one another. Uses Facebook for age verification; easily faked. Uses geo-location to ensure the matches are local. Confirming a user's identity is a problem. Often perceived as a service for casual sexual encounters.

Meet Me (13+). Friend finding app using geo-location. Users create a profile, then chat to local people immediately, and arrange to meet up. Can be configured for friendship or dating. Images you post are 'liked' or 'disliked' by others to help you find matches with others. Lower age range than using Tinder; users have the same problem with establishing a user's identity, which can be easily faked.

Snapchat (13+). Temporary messaging service. Users post pictures, videos or text. Once viewed once, they disappear from view unless saved. Screenshots can be used to save content. Sometimes used for sexting, due to a false sense of security in believing that images will not be saved to devices.

Yubo (13+). Make new friends in the local area. Users upload photos of themselves, which are browsed by other teenagers in the local area using geo-location. Mutual likes are then able to chat and meet up. Perceived by children as, 'Tinder for teens' - photos can be of anyone.

YOLO and Tellonym (13+). Users sign up to receive anonymous 'feedback' to help them improve. Commonly used for cyber-bullying - users can post unpleasant messages to one another which can be deeply upsetting.

eSafety Videos
Facebook Cafe: https://www.youtube.com/watch?v=yrjT8m0hcKU
If Facebook were real life: https://www.youtube.com/watch?v=IIY5rifojPw
Social Media experiment: https://www.youtube.com/watch?v=6jMhMVEjEQg
Tom's Story: https://www.youtube.com/watch?v=qMtcqFU1RLQ&t
Where's Klaus? https://www.youtube.com/watch?v=i4GKXsAOYZE

Continued over…

Nude Selfies
A young person is breaking the law if they take, share or possess an indecent image of themselves or another child. The National Police Chiefs' Council have made it clear that incidents involving youth produced sexual imagery should primarily be treated as safeguarding issues.

The NSPCC have excellent guidance of preventative steps and how to deal with incidents of 'sexting': https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/

If an adult requests images or videos of a child, this is grooming and must be reported to the Police via www.ThinkUKnow.co.uk

Online Sexual Exploitation
Grooming is the process by which a person prepares a child, significant others and the environment for abuse. Goals include gaining access to the child, gaining compliance and maintaining secrecy to avoid disclosure. Abusers often aim to isolate children and increase their dependence, making the child believe they have no choice. This may include bribery, gifts, flattery, sexualised games, threats, blackmail (including emotional) and desensitisation.

Signs to look out for include (but are not limited to): Secretive of phone/laptop, spending large amounts of time in the bedroom, becoming withdrawn from family/friends, being tired and personality changes. Some may suddenly have new things such as clothes or a mobile which they cannot or will not explain.

Where parents have concerns this should be report to CEOP.
https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/grooming/

Meeting up
CEOP offer the following advice for children wishing to meet other children they've met online
• Always meet and stay in a busy public place.
• Do take a trusted, responsible **adult** with you, not a friend. If the person you're meeting with isn't being honest taking a friend will put you both at risk.
• Make sure a friend or family member knows who you are meeting, where you are going and when you'll be back.
• If your instincts tell you something is wrong, it probably is. If the person you meet doesn't look like the person you've been talking to leave as soon as possible.
• Don't accept a lift from the person you're meeting.
• Stay sober.
• Take your mobile phone, keep it switched on and topped up with credit.
• Your personal belongings can be stolen - don't leave them unattended.
https://www.thinkuknow.co.uk/14_plus/Need-advice/online-dating/

Cyber Bullying
Can take place via many different routes: Text message, iMessage, WhatsApp, Social Media, Phone calls, Anonymous emails, Xbox Live, PSN. This can be worse than traditional forms of bullying, as it can continue outside of school and can take place at any time.

Where this takes place, Social Media and gaming platforms have their own reporting systems that can be used to block users. Specific guidance can be sought via bullying.co.uk

Further Reading
www.ThinkUKnow.co.uk
www.nspcc.org.uk
www.childline.org.uk
www.iwf.org.uk
www.bullying.co.uk