What are privacy settings?

Privacy settings are controls available on many websites and apps to limit who can access your profile and what information visitors can see.

When online profiles are created, it's often assumed that they will be private by default. Unfortunately this isn't always the case – many are public until the settings are changed.

How should I use privacy settings?

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'll want 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's 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're 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're 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 won't 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.

Social media platforms like Facebook and Instagram have settings which allow you to review photos and information you're tagged in before it's posted to your 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're 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're 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, you may wish to think about how this could affect their online footprint for years to come. Further advice can be found in our 'Sharing pictures of your child online' article.

Even when privacy settings are put in place, it is important to remember that information posted online is never completely private. Further information on talking to your child about sharing personal information online can be found in our personal information article.

For specific advice about privacy settings on each of the popular apps, read these guides from Internet Matters.