Australian Government
Office of the Australian Information Commissioner

Privacy tips for parents and carers

Children frequently spend time online to connect with friends, learn and be entertained. Online environments give young people the chance to express themselves and build their identities.

But children need support online, just as they do offline. Online services are designed to appeal to young people, but may not always be safe, appropriate and privacy-protective.

Sharing personal information online can be risky, so it's important to educate children on how to make good decisions and limit those risks. See our tips to help you and your children protect their privacy when they interact online.

1. Start the privacy conversation

To help your children protect their personal information and their privacy, it is essential that you talk to them about what these terms mean and why they are important.

Privacy is about protecting personal information that reveals who you are, what you do, what you think and what you believe.

Personal information includes a broad range of information that could identify an individual. This may include your name, address, email, phone number, school, date of birth and photographs.

The key message your children need to understand is that they can protect their privacy by protecting their personal information. Make sure they know how online behaviour affects their privacy. Encourage them to report anything suspicious, like unknown people contacting them or unexpected notices.

2. Discuss their digital footprint

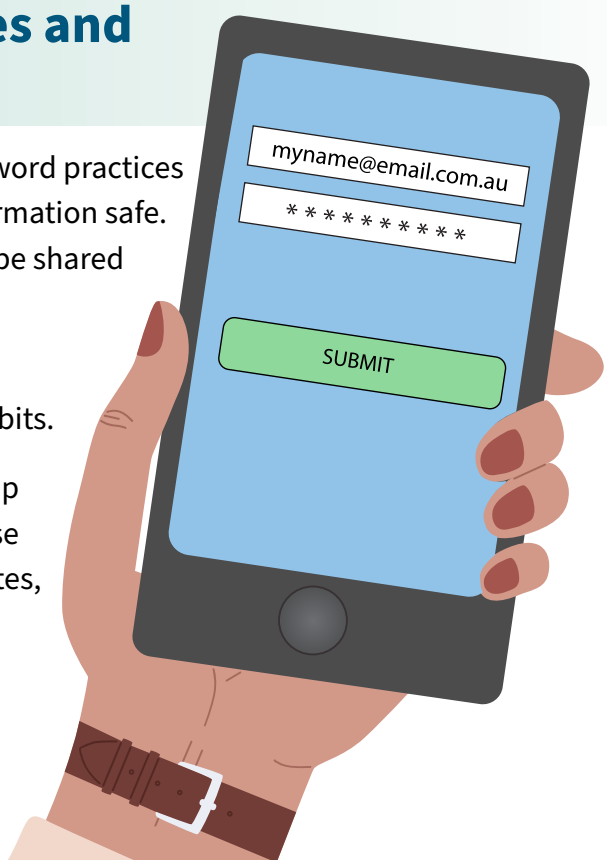
Social media and other online forums can offer a range of benefits for children, including increased connections to friends and family, and exposure to new ideas. However, children need to know that their digital footprint can last forever. It can be difficult to remove or delete information once they have shared it.

Make sure your children know the difference between the kinds of information that may be appropriate to share online and what should be kept private. There are some online situations where your children should not need to give out any personal information. However, many online services and platforms may require some personal information to create a user account to access the service.

Look carefully at what information is mandatory (such as a name and contact details like an email or phone number) and whether there is information that you do not need to provide to access the service (such as birth date, address or gender). Remember, services may use this personal information for more than just setting up an account – for example, for marketing and advertising, or other commercial purposes.

Children who understand the potential consequences of their online behaviour are more likely to make better decisions about how they share their personal information. The more personal information they share online, the greater the risk their privacy will be compromised. This is particularly important in regard to sharing their phone number, address, email, school and plans, as sharing location information may allow people to follow them.

3. Develop good password practices and use strong passphrases



It is important that your children understand that good password practices are an essential security measure to keep their personal information safe. It is also important to emphasise that passwords should not be shared with anyone, especially at school or online.

Working with your children to help them develop their own password controls will help them develop good password habits.

Create unique passphrases for all accounts which are made up of a few words and use a combination of upper and lower case letters, numbers and special characters. Avoid using birth dates, your name or the name of a family member or pet.

4. Encourage safe and smart device use

Children store a lot of personal information on their phone, tablet and laptops, so it is important they use security measures to protect this information on mobile devices.

Secure all devices with a pin lock, passcode or passphrase. Make sure your children know that someone could gain unauthorised access to their social media accounts, private message, personal photos and more if they don't secure their device. Disabling geo-location services when they are not needed is another key security measure.

Ensure children only download apps from reputable sources, especially if they are sharing location or financial information. It is also important that you know what apps and online services your child is using, and what information they have provided (or intend to provide) to access the service.

5. Tailor privacy settings and review them regularly

Privacy settings on websites, apps, online games and software are important for people of all ages, as personal information can often be collected in ways you don't expect. Adjusting settings can help you control both the types of personal information that is collected, and how it is collected, for example through webcams, microphones and cookies.

Set up privacy and other controls before children engage with a service or when they get a new device. Work with your children to adjust the privacy settings of their online accounts to limit how much and who they share their personal information with. Make time to review them regularly – like at the start of each school term.

Privacy policies and collection notices will help you understand what information is being collected about your children, and how it will be used and protected. Involve your children in checking these policies and notices to help them think about what they're swapping their personal information for. Look out for terms like 'advertising', 'marketing', 'corporate partners' and 'location tracking'. If you come across these words in a privacy policy or collection notice, see what options you have to manage this data collection in the privacy settings.

6. Be aware of online advertising

Online advertising can take a number of forms, including direct marketing and online behavioural advertising. Companies can build a detailed profile of your children just by compiling data of their online behaviour, such as the types of games, products or people they are interested in.

Controlling cookies and the use of add-ons and ad-blockers are good tools you can use to limit the amount of information about your child that can be used for advertising. You can also check whether a company gives you a way to opt out of their direct marketing.

7. Your online behaviour affects your children's privacy too

The information you share about your children on online platforms contributes to their digital footprint. Remember that once you share information, it can be used in ways you did not expect and cannot control. Before you share any information about your children, ask yourself:

- Who will see this?
- Am I comfortable with them having a photo or details about my child? Would my child be comfortable?
- Am I comfortable with the service having this information about my child, knowing that it can be used for different purposes?
- Can I protect this information using any of the tips above?

Help is always available

- Make sure your children know that if they have a problem online, they can ask for help from you, from their school or from government services. Make a complaint about how a business or organisation covered by the *Privacy Act 1988* has handled your children's personal information: oaic.gov.au/privacy-complaints. You need to complain to the business or organisation first. If they don't respond to your complaint or you're not happy with their response, you can lodge a complaint with us.
- Report child cyberbullying, image-based abuse and illegal or harmful online content: esafety.gov.au/report
- Advice for parents and carers to help children have safe experiences online: esafety.gov.au/parents
- Advice for families on protecting devices: cyber.gov.au/acsc/individuals-and-families/protect-your-devices
- Help with identify theft and related issues: IDCARE.org