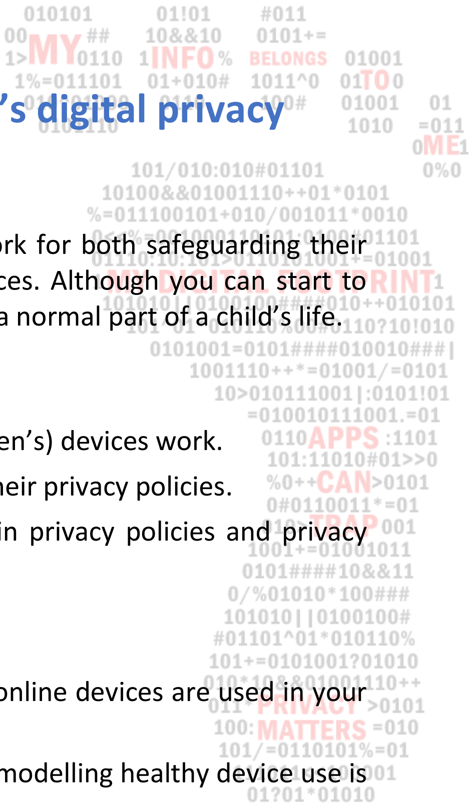
ACCM Australian Council on Children and the Media



Steps parents can take to protect their children's digital privacy (summary)

Parents can use a **three-step approach** to establish a good framework for both safeguarding their children's privacy and guiding them to make safe independent choices. Although you can start to implement these steps at any point, starting early will help it become a normal part of a child's life.

TEACH YOURSELF

- Get to know how the privacy settings on your (and your children's) devices work.
- Check apps you or your children have downloaded and read their privacy policies.
- Familiarise yourself with some of the common terms used in privacy policies and privacy settings.

BOUNDARIES, GUIDELINES, AND LIMITS

- Set up age appropriate and realistic expectations about how online devices are used in your household.
- Establish healthy digital habits for both parents and children (modelling healthy device use is a great first step).
- Stay on the same page - In dual parent households, a unified approach to the management and enforcement of rules around media use is most effective.

DO IT TOGETHER

- Joining in and sharing digital activities with your child is one of the most effective ways of protecting them against privacy risks.
- Show your child how you respond to requests for information, how you recognise any traps with apps, and how you adjust privacy settings.
- At every stage, talk your child through why and how you are making those decisions and show them how to manage privacy.

What are the privacy basics?

How you manage your privacy will be down to the device you use and the apps, platforms and programs that you use.

At the most basic level, these are the kinds of things you should be doing to protect your children's privacy:

- Check the privacy settings on the device that your child uses. Make them as restrictive as you can without compromising how the device works.
- Delete apps that you don't use very much or your children rarely open or no longer enjoy.
- Limit the number of apps that your child is allowed to have on their device. The more apps you have, the more third parties are accessing the information on your device.
- For every app, check what information it requests from your device. If it is requesting permission to use something that it really doesn't need to function, deny access.
- If your device is on the Android platform, there is a program called *AppCensus AppSearch* that can tell you what private and personally identifying information that an app is accessing and sharing with third parties (Please note: the analyses on this site are carried out under US conditions).
  You can find it here: https://search.appcensus.io/

- Read the privacy policies of the apps you decide to keep on your child's device. Check to see if they contain third party trackers. Privacy policies are often deliberately difficult to understand and very time consuming to read, so don't be put off – the more you read the easier it gets to pick out the important details.
- If your child uses a web browser such as google chrome, safari etc, find out how you can change the settings to opt out of ad personalisation. Regularly clear the saved information and any 'cookies' (the data generated by websites and saved by your web browser).
- Regularly clear your saved data, anywhere and everywhere that it is possible. Learn how you can do this on the platforms that your child uses regularly.
- If a child's app requires them to sign in, decide whether it is worthwhile. The fewer apps that have your personal details (names, emails, children's names etc) the better. If you think it is worth creating an account, make sure that it is protected by a strong password that you change regularly. Another strategy is to create a false identity that you use for creating accounts like this. This is not difficult to do and can help to protect your real-life identity.

****

MACQUARIE
University

Produced in partnership with the
Macquarie University
Department of Psychology.

accan

ACCM acknowledges the support of the
Australian Communications Consumer Action Network (ACCAN)
which funded the research for, and publication of, this document.