

Being Online at Home Tips for Parents and Carers

Privacy

When supporting your child's education at home, keep their privacy in mind, and help them establish and maintain good privacy practices.

Privacy is about protecting your child's identity. This may be their name, age, email, home address or password. It can also be more sensitive information, such as their health, wellbeing or family circumstances.

Read the [Schools' Privacy Policy](#) to understand how schools handle your child's information, and apply similar principles at home. You can request a copy of your school's privacy policy from your school.

Here are some practical tips to help you and your child maintain good privacy practices:



Passwords

Ensure your child's **passwords** to any systems they access are secure. Do not have them written down near the computer or device or save them in a document that can be accessed by others.



Logging Out

If your child is using a shared computer or device at home (e.g. a household computer or tablet), ensure that they **log out of all school systems** at the end of each session or day.



Sharing Sensitive Information

Your child may sometimes need to share **sensitive information** with school staff - for example, about their health or wellbeing. Make sure they can do so without being disturbed, and any sensitive documents they create or share are stored somewhere secure, such as a password-protected folder.



Collaboration Platforms and Applications

Your school will advise what **collaboration platforms or applications** your child may be asked to use to support learning from home. This will include advice on how to set them up to ensure your child's safety and privacy. It is very important that you follow your school's guidance. This will help ensure that the strongest privacy protections are in place at home.



Video Conferencing

If your school is using **video-conferencing**, ensure your child understands how the software works. If possible, your child should participate in videoconferencing in an open place within your home, rather than alone in a private space such as in their bedroom.



Downloading Software

Be cautious about **downloading educational software** except what your school has recommended:

- If software requires your child's personal information to be entered, make sure you read the company's privacy policy first to find out how that information is stored, and who it is shared with. If you're unsure, **check with your school**.
- Be wary of companies and products that:
 - don't have a privacy policy
 - ask for more detailed personal information than seems necessary in order to use their product
 - share user information with third parties for marketing purposes
 - store your child's information in countries whose privacy legislation is substantially different to Australia's.



Safety

When using Department or school provided equipment, including dongles, devices and laptops, please ensure that these are used for educational purposes only, to help ensure your child's safety and security.

Protecting your child and supporting them to stay safe online is a priority for parents and carers. The [National eSafety Commissioner](#) has developed a range of resources to support parents and carers to ensure their child's safety and privacy online, including:

- [parent webinars](#),
- tips on [how to report cyberbullying](#) and
- [online safety kit for parents and carers](#).

Security

- Make sure you have anti-virus software installed on your computers or devices at home and this software is up to date.
- Download and install any updates for other software on your computers or devices at home. These updates often include 'patches' that fix security vulnerabilities and other bugs.
- When online, ensure that any links you or your child click on are genuine. 'Phishing' is when someone sends you a link that looks ok, but is actually sending you somewhere dangerous or inappropriate. These links may look like they come from your school, a software provider, the bank, the government or from apps your child uses. More tips can be found on the [ScamWatch website](#) or from the [eSafety Commissioner](#) website.

Copyright

Here are some practical tips to help you and your child maintain good copyright practices:

Use existing free sources of content

- There are many free online streaming content services where students can access content without having to download or make a copy of it. Examples include ABC iView, ABC Education and YouTube Kids.
- The Department of Education and Training has purchased a licence which provides all Victorian Government teachers and students with access to [ClickView](#), a platform that hosts thousands of educational video resources and learning activities. Your school can provide your child with a login to enable them to watch material hosted on ClickView at no cost.

Link to content, rather than download it, where possible

- If your children need to access or share internet content, advise them to use links rather than a downloaded copy where possible.
- If you don't have internet access at home or limited access, contact your school who may be able to provide you with copies of materials.

Access school subscriptions from home

- The Department provides access to a range of software that schools can use to support teaching and learning, including [Webex](#), [ClickView](#), [Stile Education](#) (for students in years 7-10), [G Suite for Education](#), [Microsoft O365](#) and [Minecraft: Education Edition](#). Your school will advise you on what software your child will use to support their learning from home.
- Students often already have access to school-provided subscriptions that are useful for supporting learning from home, for example Reading Eggs, Mathseeds and HOTmaths. Check what is already available from your school before signing up to anything new.