

5. Comply with any direction to load or update software that controls access to content and ensure that this software is in operation.
6. Maintain the Device in good working order and ensure that the Student uses the Device in accordance with the Device manufacturer's instruction.
7. Ensure the Device is not misused or tampered with by any person.
8. All times keep the Device under his or her personal control both during and outside school hours.
9. Notify the School Representative immediately following any loss or damage to the Device.
10. Ensure the Device is returned to the School at the end of the Remote Learning Period or within 5 business days of the School requesting the Device be returned.
11. Understand that the school is limited in the technical support that can be offered, due to technicians working remotely. If there is any issue with the device, it may not be able to be actioned.

The Recipient (parent/carer) agrees that:

1. The School can request the return of the Device at any time.
2. In the event the Device is lost or damaged (e.g. if loss is caused by leaving the Device in an unlocked or unattended vehicle, except in a locked boot or a locked vehicle, or some other negligent act), then the Recipient may not be eligible to borrow a replacement Device from the School. The School can invoice parents for any resulting loss or repair costs.
3. On the completion of the Remote Learning Period the Device will be returned to the School in good repair, condition and working order, ordinary wear and tear excepted.

Signed by Recipient:

Signed on behalf of school:

Date: ____ / ____ / ____

Date: ____ / ____ / ____

We will contact you about collection of a suitable device, as well as provide passwords for the device.

APPENDIX 1: Being online at home: tips for parents/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 information, and apply similar principles at home.

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

- 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.

- 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.
- Your child may sometimes need to share **sensitive information** with their teacher or other 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.
- Your child's teacher 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.
- 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.
- Avoid downloading **educational software**, except what the school has approved or recommended for *Learning from Home*.
- 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, you can **email the school to check**.
- 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 the 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 School has compiled a list of useful resources to support parents and carers to ensure their child's safety and privacy online. See [this link](#).

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.
- 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 child's teacher may provide your child a ClickView 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.

Access school subscriptions from home

- The Department provides access to a range of software that schools can use to support teaching and learning. Your child's teacher 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. You will not need to sign up to anything new.

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 notified 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](#).