

Equipment Loan Agreement

DETAILS

| | |
|---|--|
| School: | Casterton Secondary College |
| School Representative: | Renee Jukes |
| School Representative contact details: | casterton.sc@edumail.vic .gov.au 03 5581 1588 |
| Recipient: | |
| Student: | |
| Device: | |
| Model/Serial Number of Device: | |
| Remote Learning Period | |

In consideration of the School, at the request of the Recipient, making available the Device to the Student for educational purposes during the Remote Learning Period, the Recipient (parent/carer of the student) agrees to the following terms and conditions:

The Recipient agrees to:

1. Supervise the Student's use of the Device at all times during the remote Learning Period and comply with the school's **Acceptable Use Agreement**.
2. Ensure that the Device is only used for access to education related sites and not used to access inappropriate content. Refer to attached guidelines on safety.
3. Comply with any direction to load or update software that controls access to content and ensure that this software is in operation
4. Maintain the Device in good working order and ensure that the Student uses the Device in accordance with the Device manufacturer's instructions
5. Ensure the Device is not misused or tampered with by any person
6. All times keep the Device under his or her personal control both during and outside school hours
7. Notify the School Representative immediately following any loss or damage to the Device.
8. Accept responsibility for the payment of a \$100 insurance excess, in the event of lodging an insurance claim.
9. 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.

Casterton

Secondary College

27 Mount Gambier Road, Casterton VIC 3311
Phone: (03) 5581 1588
Fax: (03) 5581 1518
Email: casterton.sc@edumail.vic.gov.au
www: www.casterton.vic.edu.au

The Recipient agrees:

1. The School can request the return of the Device at any time.
2. That 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.
3. To assist the School with respect to the lodgement of an insurance claim where requested.
4. That 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: |

Appendix 1: 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 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.
- Be cautious about downloading **educational software** except what the 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, you can **ring the school (PH: 5581 1588) 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 **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.**

Copyright

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

Use existing free sources of content

- The Department provides access to a wide range of learning materials available from the **FUSE website.**
- 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 child's teacher will 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.
- If you don't have internet access at home or limited access, please let your child's teacher and they can organise providing you with copies of materials.

Access school subscriptions from home

- The Department provides access to a range of software from the **FUSE website** 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 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, for example Reading Eggs, Mathseeds and HOTmaths. Check what is already available from your school before signing 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 updates for other software on your computers or devices at home. These updates often include 'patches' that fix security vulnerabilities and other bugs.
- Unsolicited technical support is a key method for scammers to gain access to your computer and your confidential information. Do not install any software at the request of someone posing as a representative of a company where you have not actively requested support, whether you are contacted by phone or by e-mail.
- 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.