

1-to1 Student Learning Device Policy

Contents

Preferred ownership/transfer model

Privately owned devices

Optional peripherals

Guidelines for participation

Role of parents/carers

Insurance

Loan/replacement

Caring for 1-to-1 devices

Appearance and personalisation

Software licencing

Internet usage

Users and security

Virus protection

Non-school applications and files

Web 2.0 applications

Technical support

Power supply management

Backup/recovery

Additional student consumption

Preferred ownership/transfer model

The 1-to-1 device will be part of a leasing arrangement between the school and *equigroup*.

The school will make the device available to the student during regular timetabled classes within the school, subject to the classroom teacher deeming its use to be appropriate at that time.

The device may not leave the school under any circumstances. The school will make a limited number of school owned devices available for borrowing by students when required, with permission granted on a case-by-case basis.

When the student exits the school the device is retained by Croydon Community School, erased, and prepared ready for use by another student.

Privately-owned devices

Privately owned devices are not to be connected to the school network unless there is special authorisation from the IT Manager or Principal to do so. Privately owned devices that do not meet anti-virus and operating system patching requirements pose an unacceptable risk to other devices on the school network and broader Department of Education and Training (hereafter known as "DET") network.

Optional peripherals

Croydon Community School will not provide or specifically recommend any additional peripherals as part of the 1-to-1 program unless they are a class requirement, however, parents/carers or students may purchase these themselves. Program support and warranty will not apply to these peripherals.

Peripherals may include:

- Mice
- Headphones
- USB backup/storage devices
- External DVD drives

Guidelines for participation

As part of Croydon Community Schools commitment to provide access to computers, all enrolled students attending the Croydon site will have access to a 1-to-1 student learning device whilst in class at school provided that the student and parent/carer have signed the Croydon Community School Acceptable Use Agreement for internet and digital technologies and the Student Laptop Agreement.

Role of parents/carer

Parents/carers should ensure that they and their child understand and are familiar with the Croydon Community School Acceptable Use Agreement for internet and digital technologies and the Student Laptop Agreement. These agreements should be signed and returned to the school as quickly as possible to avoid unnecessary delays in a device being allocated and configured ready for use.

Insurance

The Acer TravelMate B115 1-to-1 student learning device will be insured through JUA Underwriting Agency Pty Limited. The insurance shall cover any unforeseen physical loss of, or damage to the device caused by; Fire, explosion or lightning; Burglary and theft; Malicious or accidental damage; Impact; Electrical and electronic breakdown; Storm, flood, water; Power surge, low voltage or mechanical damage whilst at the insured situation (“177-181 Mt Dandenong Road, Croydon VIC 3136”).

Each insurance claim will be subject to an excess of \$100. This will be paid by the school except in cases where the school forms the belief that a student significantly contributed to the loss or damage.

If loss or damage occurs is the fault of a student and is not covered by insurance, the student will be responsible for the total cost of replacing or repairing the device.

Loan/replacement

The school will make a limited number of devices available for use by students at any time their device is unavailable. Access to loan/replacement devices will be granted on a case-by-case basis and a prior history of poor care may prevent a student from receiving a loan/replacement device.

The loan/replacement devices may not necessarily be the same make and model as the regular student learning device.

All student learning devices (SLDs) will have a next business day warranty to minimise downtime however there may be cases where parts are not available and repairs may take longer.

Caring for 1-to-1 devices

For the protection and longevity of devices it is important that the following conditions are adhered to. Not caring for the student learning device properly could void its warranty.

- Avoid placing objects on top of the device because pressure from books and other objects can damage the screen and other components
- Do not grab or squeeze the device because this can also damage the screen
- Never leave your device in unsupervised areas during the school day. When not in use your device should be returned to the laptop trolley located in the Advisory classroom. Devices left unsecured will be confiscated to avoid exposure to loss or damage
- See Appendix 1 for Guidelines for students on caring for their 1-to-1 device.

Appearance and personalisation

The physical appearance of the student learning device must not be altered in any way. This includes the protective skin. Alterations will be considered as damage and the student will be responsible for reimbursing the school for any costs incurred in returning the device to its original physical appearance.

Software licensing

Software preloaded on the device is subject to license conditions and must not be distributed or deleted without written permission from the IT Manager or Principal.

Periodically new software titles may become available and this may require the student learning device to be re-imaged. In the event of this, students will be notified and asked to backup any data stored outside of their H: drive prior to the re-image taking place.

Internet usage

Use of devices by students is governed by the Acceptable Use Policy that students and parents/carers agree to for use of ICT within the school. Parents/carers are required to familiarise themselves with the Acceptable Use Policy.

Inappropriate use of the internet is unacceptable and is subject to disciplinary action and exclusion from the school network and resources.

Resources for parents and teachers are available at:

- **Office of the Children's eSafety Commissioner** - <https://www.esafety.gov.au/>
- **Stay Smart Online** - <http://www.staysmartonline.gov.au/>
- **ThinkUKnow** - <http://www.thinkuknow.org.au/>

Users and security

Students will access their device using their school-provided network login. In the event that they forget their password students will need to contact IT Support within the school.

Students are not permitted to allow other students to log onto their device.

Software titles may be installed by the student onto their device as long as it is relevant to their education/ILP and is suitably licenced. To achieve this, students will be granted administrator rights on their student learning device. Students found to have installed inappropriate software titles will have their administrator rights revoked and the offending software titles will be removed.

So that personal information is protected in the event that the device is lost or stolen it is important that students maintain a "Complex 7" password. Complex 7 passwords must have between seven and 32 characters, and one character from at least three of the following sets:

- uppercase letter (A-Z)
- lowercase letter (a-z)
- numeral (0-9)
- special character such as ()~`#\$*&

Virus protection

Viruses have the potential to severely damage and disrupt operations within the school and DET's computer networks. As students have the right to add software to their device and connect to the internet, they should take all steps to protect the school and DET's computer network from virus attacks.

The student learning devices have Microsoft System Center Endpoint Protection installed on them. The virus software will be automatically updated from the network.

Students are recommended to:

- Protect their devices from virus attacks by scanning for viruses at least weekly. Microsoft virus definition updates are managed automatically by the school network.
- Consider running virus scans regularly after accessing the internet or e-mail or opening a file from a removable media source (e.g. USB stick or external hard disk).
- Not open any files attached to suspicious or unknown e-mails.
- Exercise caution when downloading files from the internet. Save the files to the device's hard disk and run the virus scanner on the file before opening it.
- Delete chain and junk e-mails. Do not forward or reply to any of these.
- Never reply to spam. Spam e-mail messages can contain elements that notify a third party of the legitimacy of an email address and then add the recipients to the spammer's database.

Under no circumstance may a student remove Microsoft System Center Endpoint Protection from their device or disable it. Students found to have done this will lose use of their device immediately.

Non-school applications and files

Software, including music, movies and games will be allowed for educational and recreational reasons, provided copyright and license obligations are met. Personal MP3 and other music files may be stored on the device provided that student is licenced to do so.

Downloading music, games and videos from the internet during school hours is prohibited except where directed by a staff member. Students are permitted to listen to digital music and/or participate

in games on their device while at school where permission has been given by the classroom teacher for an educational purpose.

It is the student's responsibility to ensure that there is enough hard drive space and memory available to engage in all educational requirements.

Students must ensure that any games, music videos or movies are within the required standards of ratings for their age (under 15 years PG or G only, over 15 years M may be added, MA or MA+ are not acceptable by any students).

Web 2.0 applications

Students must abide by the schools Acceptable Use Policy whenever the schools equipment or services are involved.

The Acceptable Use Policy contains specific requirements to ensure student safety.

- Students must keep themselves and friends safe by not handing out personal details, including full names, telephone numbers, addresses, images and passwords
 - Students should be respectful in how they talk to and work with others online, and never participate in online/cyber bullying or harassment
- Students should use the technology at school for learning, use the equipment properly and not interfere with the work or data of another student.

Technical support

The student learning devices will be supported by the school IT Manager and DET Specialist Technician during school hours. Support can be obtained by sending an email to the IT Manager or by visiting the IT Office.

Technical support staff will attempt to resolve/remediate issues where possible however in some cases where a resolution cannot be reached within a reasonable timeframe technicians will re-image the device. The student will be provided with the opportunity to ensure that all school work is present in or has been backed up to their H: drive prior to this occurring.

As students have administrator rights on their device they are strongly advised to proceed with caution when installing new software or using the internet.

Power supply management

Students are to return the device to the classroom laptop storage trolley at the end of each class and connect the power cord so that the device can recharge. It is the students' responsibility to ensure that the device is always charged and ready for use.

Backup/recovery

Students are encouraged to save all school related work/data in their H: drive. The H: drive is the students own secure workspace that can only be accessed by them (*and members of staff*) from their student learning device or any other networked computer in the school. Data saved to the H: drive whilst the device is connected at school is automatically transferred to the server and backed up. A copy of this backup is replicated nightly to another Croydon Community School site. Data saved in H: whilst the device is offline will be automatically transferred to the server next time the device is connected.

The H: drive has a 25 GB (25,600 MB) storage limit. If students require additional space a request can be made to the school IT Manager. Students must be able to demonstrate a genuine need and must not have data not related to their education/ILP within the drive for the request to be approved.

Data stored outside of the H: drive such as in Documents, Pictures, Music and on the Desktop is the students responsibility and must be backed up manually by the student.

Printing - additional student consumption

All students at the school start each year with a \$20.00 print quota allocation with monochrome pages being charged at 10c and colour pages charged at 20c. When a student reaches \$0.00 they are unable to print. Students should speak to the IT Manager if they have insufficient quota and require a top-up.

If the IT Manager forms the belief that the student has not been printing responsibly a quota top-up may be temporarily withheld or alternative strategies put in place to assist the student with responsible printing.

All printer usage is monitored and recorded.

Internet download quotas are not currently enforced at the school however all usage is monitored and recorded.

Appendix 1 – Caring for your 1-to-1 device

Packing away your device

- Store your device in the laptop trolley upright with the power plug facing towards you.

Handing your device

- Try to avoid moving your device around when it is switched on. Before switching on, gently place your device on a stable surface and then switch on
- Devices should always be shut down before being put into the laptop trolley.

Operating conditions

- Don't place objects near the top of your device and never carry it around while it is turned on
- Avoid exposing your device to direct sunlight or sources of heat
- Avoid exposing your device to dust, dirt, rain, liquids or moisture
- Avoid exposing your device to heavy shock or vibration.

LCD screen

- LCD screens are delicate – they don't like being poked, prodded, pushed or slammed. Apply as little pressure as possible when using the touch screen
- Never pick up your device by its screen
- Don't slam the screen closed
- Be gently when putting your device down.

To clean your LCD screen

- Switch off your device
- Lightly dampen a non-abrasive cloth with water and gently wipe the screen in a circular motion
- Do not directly apply water or cleaner to the screen
- Avoid applying excessive pressure to the screen.

AC adaptor

- Connect the power plug only to your device and always use the plug hanging in line with your laptop trolley slot. Avoid using power cables from other slots as this usually ends up causing cables to become tangled
- When unplugging the power plug, pull on the plug itself rather than the cord.

Keyboard

- Gently brush your keyboard with a soft bristled paint brush or similar to remove dirt
- If any key tops are missing or keys are in a damaged state, take your device to technicians to be repaired immediately. A single key top can often be replaced but continuing to use the keyboard with a missing key top can result in having to replace the entire keyboard.

Case cleaning

- Use a non-abrasive cloth
- Spray cleaner on to cloth to moisten, but do not spray the device directly. Rub gently.