



Device User Agreement 2025

General

The Computer systems operated at the Coomandook Area School are for the purpose of supporting the teaching and learning program.

Coomandook Area School recognizes that computing skills and in particular electronic information research skills are essential for students as technologically literate citizens. Access to computers, the school's curriculum network and the Internet is provided for the purposes of educational learning and research. Access to the facilities entails responsibility. The purpose of this agreement is to provide rules for the appropriate use of these facilities. Students and caregivers must sign the computer use agreement and return to the students homegroup teacher before gaining access to the school network.

General Computer Use.

The School network is a restricted access computer system. It is a breach of this user agreement to:

- Install or operate any computer software or computer hardware without the prior approval of the network manager.
- Use or possess any computer hardware or computer software that can be used to avoid or remove any access restrictions placed on the computer system by the network manager.
- Obtain or use any user names or passwords except those issued to an individual by the network manager.
- Wilfully damage any computer hardware or software.
- Display, Send, Store, Access, or Retrieve any offensive or inappropriate material on the school computer system.
- Access or destroy any data or hardware belonging to another individual or the School.
- Modify computer hardware or computer software in any way without the prior approval of the network manager.
- Use the computer system to engage in or enable others to engage in copyright infringement.

STUDENTS ARE NOT PERMITTED TO HAVE IN THEIR FOLDERS OR ON ANY PORTABLE STORAGE DEVICE:

- software such as games, utilities, system hacking utilities or executable files, Mac or PC
- files containing sound or video sources – except for subject specific purposes eg information technology
- downloaded Internet files not subject based etc – this includes music and video files.
- hidden files

Students whose folders or storage devices are found to contain any or the above may have their access to the network removed immediately and a cost may be incurred to reinstate their account.

User ID and Passwords

The password protects a user's folder or directory. Password confidentiality is a serious matter and it is most important that the student does not divulge his/her password to anybody else.

- All individuals are given unique user names and passwords to access the school computer systems
- It is essential that users keep their user names and passwords confidential.
- Students must not divulge their user names and passwords to anybody under any circumstances. This includes and is not limited to School Staff members.
- Student user names are linked to student's individual Internet and printing credits.
- No student is to access another student's folder on the system or allow other students to access theirs.

Use of the Internet

The Internet can be a valuable resource. It often provides ready access to up to date information. Students need to remember that:

- the Internet is provided for educational purposes
- the source of the material needs to be checked for its worth. Remember anybody can publish information on the Internet.
- All Internet activity is logged and audited
- Downloading of software is NOT permitted

The school's Internet is filtered. Known pornographic, violent, hate sites etc are blocked. However, if a student encounters such a site, they need to exit that site immediately.

Using the school's network to engage in commercial activity is strictly prohibited. Students are automatically assigned a department email address. This service is monitored to ensure appropriate language is used. **This is the only email account students are to use at school.**

School Owned Laptops:

Students from years 7-12 are issued school owned laptops and a laptop bag. Students are to ensure their laptop is fully charged overnight so it is ready for the beginning of each day.

Any student in years 11 and 12 are welcome to bring their own laptop (BYOD) – please see below. Students are expected to look after their device and always carry it around school in the bag provided and report any issues they have to IT Support.

Use of Privately Owned Devices (BYOD – bring your own device)

Before any private laptop or device is used within the school it will need to be approved by the IT Support for its suitability. Devices are to have current **Antivirus software** loaded and this needs to be kept up to date. The use of the laptop or device will be permitted as long as the user follows the computer user policy as outlined in this document.

All devices connecting to the schools wifi are to have software installed to monitor the use of the internet.

All students who are enrolled in a DfE school are entitled to have the Microsoft Office Package installed on their personal device while they are enrolled at a school. Please see the IT Support for installation.

School printers are required to be set up on BYOD devices to enable students to print.

Hot spotting your phone for internet purposes is NOT allowed while on the school site. School Wifi access is granted to all students and this is the only internet access students will need.

USB's and Backing up

Students are not to bring personal USB or storage devices from home. Any student found using a personal USB will have it removed and computing privileges may be removed. Students USB's are purely for school work, no other file, movies etc are permitted to be brought to school. Students are highly encouraged to use one drive to back up all their work.

Students are reminded to back up their work in at least 3 different places. It is recommended you save your work in One Drive, on your laptop/notebook, and to the school network. This is especially important for senior school students.

Viruses

Users are asked to check files on storage devices for viruses before using them in a school environment. Cortex antivirus program is installed on each school computer. Any attempt to introduce a virus to the School systems deliberately will incur harsh penalties.

System security/hardware configuration

If a student identifies a security issue on the school's network or the Internet, they must notify IT Support or a teacher immediately. They are not to demonstrate the problem to others.

Students are prohibited from accessing the system in an unauthorized way or assisting others to do so. They are prohibited from altering system files, system configurations, desktops, folders (except their own) and other technical data.

Monitoring User Activity

While confidentiality and privacy is a high priority, the school reserves the right to monitor network and computer activity. This will involve monitoring of:

- Users computer screens
- Files in user's directories
- Files on portable storage devices
- Internet activity
- E-mail
- General behavior and respect for the computing resources throughout the site

Damage

Students may be required to pay for, either wilful or accidental, damage caused to school owned computers, iPads, 3D printers, hardware and equipment.

These consequences apply regardless of the student's area of study. Some subjects require computer access and in these cases the consequences are high to protect other users.

Printing

Students are given a \$25 printing quota at the start of every year. Students are permitted to print school assignment documents only. Students have access to colour printing however are asked to limit the amount of drafts printed before a final copy is handed up.

Any student who breaches the printing rules will have their printing account disabled.

If a student runs out of printing quota, they will need to top up their account by bringing in additional money for their printing to the front office.

Office 365

Through the department students will have access to Office 365. Office 365 provides access to Microsoft services online, including Word, Excel, PowerPoint, Teams and One note. Office 365 services provided by the department are only to be used for curriculum purposes and not privately. With online services there is always an increased risk of loss and damages to personal computers or mobile devices including applications, information and data stored on processed or accessed in conjunction with Learnlink O365. Students are reminded that they are to back up their own computer environment, including information and data before downloading and installing Office 365 Pro Plus.

iPad

The use of an iPad is to be for school purposes only, and only to be used under the instruction of a teacher. Students are to not attempt to download any apps on any device.

3D Printer

The 3D Printers and Laser cutters are to be used strictly only under the instruction and supervision of the tech teacher. Misuse of this technology will result in an account for the cost of materials wasted.

Mobile Phones

Refer to new DfE policy for mobile phone use on department sites.

It is regretted that an agreement document like this is needed but past experience has shown that clear guidelines and consequences for inappropriate computer use must apply and be well understood by all users if the computing resources are to be used for the benefit of all users.

We encourage students, parents and community users to support us in the effective management of these resources.

COMPUTER USE AGREEMENT TO BE RETURNED TO FRONT OFFICE – STUDENTS ARE NOT PERMITTED TO TAKE A LAPTOP HOME UNTIL THIS IS RETURNED.

I have read and agree to the terms of the computer use agreement.

Student name: _____ Parent/ Caregiver name: _____

Signed: Student

Parent/ Caregiver