



\$300 Student Equitable Access Device Charter



Pimlico SHS has implemented a Bring Your Own Device program for students in Years 7, 10, 11 and 12 in 2024. In order to enable students and families with limited resources to engage with the program, Pimlico has co-contributed for devices to be on-sold to students and families that can demonstrate financial hardship

To be eligible for this program, students must be able to demonstrate financial hardship to the relevant year level Deputy Principal, be up to date with the current year’s SRS fees, and complete this form. The device will be provided to students under a lease-to-buy program, where students and families are asked to pay the full \$300 cost up-front. The allocated student will gain possession of the laptop and become responsible for its care and maintenance. However, the school will manage the device’s BIOS and operating environment to help reduce theft. When a student graduates, or otherwise ends their schooling at Pimlico SHS, the school operating environment and all file contents will be removed and the device returned to the student as their personally owned machine.

Students and families/caregivers are asked to lend their support to this very valuable program. Strong support from families and caregivers is paramount to ensure the program is successful and that students are connected any time, anywhere to their learning.

DEVICE

The device that has been purchased by Pimlico State High School for the equitable access program is a Lenovo 13w Yoga R5

Lenovo 13w Yoga R5 (supplied by Queensland Computers) contains:

- AMD Zen3 Ryzen5 5625U processor
- 13.3” touch screen and stylus
- 8GB RAM
- 256GB M.2 SSD
- HDMI port
- Front and rear facing cameras
- 2x USB-C & 2x USB-A ports (1x USB-C for charging)
- “Flip” chassis allowing use as a notebook or tablet
- No Ethernet (RJ45) port
- 3 years warranty (no ADP) beginning June 7th 2023
- MOE5 Win10 20H2

The device was chosen by the department based on a number of criteria including portability, battery life, hardware capabilities, overall cost and warranty.

LEASE EQUIPMENT

To participate in the Equitable Access Program, families and/or guardians are required to make a one-time payment of \$300 to initiate the lease. This will partially cover additional costs incurred by the school in providing and supporting the device. Funding has been made available by the State Government for the implementation of the program to supply the devices to Pimlico State High School for \$500, with Pimlico SHS covering the remaining \$200.

By paying the \$300 fee, students and families will obtain the following:

ITEM	COST
Lenovo 13w Yoga R5	Included
Stylus	Included
Power Adaptor	Included
Windows operating system and license	Included

For the duration of the student's enrolment, students and families will also obtain the following support:

ITEM	COST
PSHS IT support & help desk	Included
Microsoft Office suite	Included
Windows 10 Managed Operating Environment	Included
Blue Coat internet filtering	Included
BIOS password protection	Included

The following items are **not included** in the \$300 fee, and students should obtain for themselves:

ITEM
Computer mouse
Other subject-specific software
Carry Case or Bag
Accidental damage protection and insurance

EQUIPMENT OWNERSHIP

All devices used in the program are the property of Pimlico State High School and the allocated student under a lease arrangement until the student graduates or otherwise leaves the school.

If the student leaves the school, transfers to another school, moves interstate or overseas, the device must be brought to the school as soon as possible for the transfer of ownership to occur. If the device is not returned, the device will become unusable due to the school-managed protection. The school may require access to the device upon request to protect the device and school network from unexpected events, for example from malware.

The school retains partial ownership of the device in order to facilitate the Managed Operating Environment. At the end of the lease period, the device is to be brought to the school IT support & help desk to have the Managed Operating Environment and other school-provided software and protections removed. After this process has occurred, the device will be written off from the school's asset register, and ownership of the device will transfer wholly to the allocated student.

The student should backup their data as all data will be wiped from the machine in the process of transferring ownership and restoring the operating system to Windows' default settings.

DEVICE CARE

The student is responsible for taking care of and securing the device and accessories. Damage to the device or hardware are the students financial responsibility to repair. Software errors may be able to be solved with the support of the Pimlico SHS IT support & help desk on a case-by-case basis.

Accidental and Non-Accidental Damage

Be aware that both accidental and non-accidental damage are not covered under the device's warranty. Protection of the device against damage or loss, such as through an insurance policy which protects against accidental damage or theft is the sole responsibility of the student or family.

Examples of accidents include:

- Accidentally dropping the laptop, which results in physical damage to it.
- Accidentally spilling liquid over the keyboard. When a liquid spill occurs and is rectified quickly, it is possible to limit damages to the notebook. Otherwise, factors such as rust damage and corrosion caused by the liquid can cause further issues.

Other examples of non-accidental damage can include:

- The laptop falling from a shelf due to the power cord being pulled, resulting in damage to the device. This would be considered carelessness.
- “Accidentally” stepping on the laptop while on the floor or jumping on it when in bed. These incidents would be considered carelessness, if not deliberate.
- Leaving the notebook unattended and as a result it was damaged by someone or something else other than the user or assigned owner.
- No explanation whatsoever can be provided for how the resulting damage occurred.
- Repeating cases for the same laptop which may have previously been termed accidents.

For accidents that result from a fault or manufacturing defect, rather than accidental or willful damage, see information below concerning clarification of warranty conditions for faults.

Theft and Loss

If the device is stolen outside the school, the family\caregiver will need to report the incident to the police and ensure they have the following documents when informing the school:

- The police crime number and
- Statutory declaration (usually completed with the police)

On receipt of the necessary documentation, the school and student will initiate recovery procedures. Should a device be unrecoverable, the cost of replacement falls on the student or family, and the student may not be eligible for a second device under this program due to limited supply.

Warranty Claims and Conditions

Warranty claims for repairs or replacements can be pursued when the product has clearly failed due to a manufacturing defect. These incidents are covered under the warranty that is guaranteed to consumers under ACCC rights and guarantees upon the purchase of the device.

The school retains purchasing information of the devices from the supplier and in its asset-management system, and can provide information to support a warranty claim made by a student or family. Warranties for the provided devices extend three years from their date of purchase by Pimlico State High School.

DATA SECURITY AND BACK UPS

Students must understand the importance of backing up data securely. Should a hardware or software fault occur, assignments and work that has taken a considerable time to prepare may be lost.

The student is responsible for the backup of all data. While at school, students are able to save data to the school’s network which is safeguarded by a scheduled backup solution. They are also able to save data locally to their device for use away from the school network, or over the internet using school-provided Microsoft OneDrive services. The backup of this data is the responsibility of the student and should be backed-up on an external device, such as external hard drive, a USB drive, or OneDrive.

Students should also be aware that, in the event that any repairs need to be carried out, the contents of the device may be deleted and the storage media reformatted.

ACCEPTABLE COMPUTER AND INTERNET USE

Upon enrolment in a Queensland Government school, familial or caregiver permission is sought to give the student(s) access to the internet, based upon Department of Education policy. This policy also forms part of this Equitable Access Charter. The acceptable-use conditions primarily apply to the use of the device and internet while on the school grounds. However, while students have elevated permissions to the device and less-restrictive internet access while not on school grounds and not connected to the school network, these conditions still apply.

Communication through school-provided internet and online communication services must comply with the Code of Conduct, available on the school website.

In adhering to the acceptable use of ICT and Code of Conduct, students should not:

- create, participate in or circulate content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- disable settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard
- use unauthorised programs and intentionally download unauthorised software, graphics or music
- intentionally damage or disable computers, computer systems or Queensland Department networks
- use the device for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.

Note: Students' use of school internet and online communication services may be audited at the request of appropriate authorities for investigative purposes surrounding inappropriate use.

MISUSE AND BREACHES OF ACCEPTABLE USAGE

Students should be aware that they are held responsible for their actions while using the internet and online communication services. Students will be held responsible for any breaches caused by other person(s) knowingly using their account to access internet and online communication services.

The misuse of internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

Digital citizenship

Students should be conscious creators of the content and behaviours they exhibit online and take active responsibility for building a positive online reputation. They should be conscious of the way they portray themselves, and the way they treat others online.

Students should be mindful that the content and behaviours they have online today are easily searchable and accessible. This content may form a permanent online record into the future.

Interactions within digital communities and environments should mirror normal interpersonal expectations and behavioural guidelines, such as when in a class or the broader community.

Families are requested to ensure that their child understands this responsibility and expectation.

ACCOUNTS AND PASSWORDS

The equitable access device outlined in this charter will be accessed using the student's school MIS username and password as part of the provided device management. The following password guidelines should be followed to protect the device against unauthorized access and theft:

- Passwords must not be obvious or easily guessed; they must be kept confidential, and changed when prompted or when known by another user.
- Personal accounts cannot be shared.
- Students should not allow others to use their personal account for any reason.
- Students should log off at the end of each session to ensure no one else can use their account or device.

PRIVACY AND CONFIDENTIALITY

It is important that students do not publish or disclose the email address of a staff member or student without that person's explicit permission. The student should not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. It should also be ensured that privacy and confidentiality is always maintained.

INTELLECTUAL PROPERTY AND COPYRIGHT

Students should never plagiarise information and shall observe appropriate copyright clearance, including acknowledging the original author or source of any information used. It is also important that the student obtain all appropriate permissions before electronically publishing other people's works or drawings. The creator or author of any material published should always be acknowledged. Material being published on the internet or intranet must have the approval of the principal or their delegate and have appropriate copyright clearance.

MONITORING AND REPORTING

All Students should be aware that all use of school internet and online communication services can be audited and traced to the account of the User.

All material on the device is subject to audit by authorised school staff. If at any stage there is a police request, DoE may be required to provide the authorities with access to the device and personal holdings associated with its use.

CYBERSAFETY

If a student believes they have received a computer virus, spam (unsolicited email), or they have received a message or other online content that is inappropriate or makes them feel uncomfortable, they must inform their teacher, family and/or caregiver as soon as is possible.

Students are encouraged to explore and use the 'Cybersafety Help' button to talk, report and learn about a range of cybersafety issues.

Students must seek advice if another user seeks personal information, asks to be telephoned, offers gifts by email or asks to meet a student.

Students must never initiate or knowingly forward emails, or other online content, containing:

- A message sent to them in confidence
- A computer virus or attachment that is capable of damaging the recipients' computer
- Chain letters or hoax emails
- Spam (such as unsolicited advertising).

Students must never send, post or publish:

- Inappropriate or unlawful content which is offensive, abusive or discriminatory
- Threats, bullying or harassment of another person
- Sexually explicit or sexually suggestive content or correspondence
- False or defamatory information about a person or organisation.

Families, caregivers and students are encouraged to visit the Department's Cybersafety and Cyberbullying document at <https://www.qld.gov.au/education/schools/health/cybersafety/cybersafety-qss>

SOFTWARE AND UPDATES

The student should ensure that all provided software is kept up-to-date through automatic and scheduled updates. If you are experiencing difficulties related to software updates, try restarting your machine to allow pending updates to install.

The software loaded on the device is licensed to the Department of Education or the school. The family or caregiver must ensure that the software is not copied, deleted or transferred, without prior written consent from the school. Unauthorised use may breach copyright laws and the family or caregiver may be held liable for any damages incurred.

ELEVATED ACCESS

Devices have elevated permissions which would provide the ability to complete tasks such as installing home items including home printers, cameras and/or licensed software.

This access may allow further permissions above and beyond those available on other MOE (Managed Operating Environment) built workstations and devices. Students should not misuse these privileges. The misuse of this access may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

If given elevated access, students have the ability to install additional software onto the device. However, only licensed software can be installed. The student must hold a valid license for any software installed and the license must be appropriate for installation on the device.

WEB FILTERING

The Department of Education operates a web filtering system to protect students and restrict access from malicious web activity and inappropriate websites.

The DoE Web filtering system is installed on departmentally-owned computers, including Computer for Student (CFS) devices. There is also a locally installed Web filtering client, which resides on the device and is active when using a non-DoE wireless connection to ensure filtering is always applied.

When students are connected through DoE managed networks, they will have a high level of filtering applied.

When students use their devices at home, the filtering system (BlueCoat Unified Agent), continues to function.

Two levels of filtering are available at home to provide students with a less restrictive internet access than at school but still a greater level of protection against access to inappropriate content and web sites. Families may select which level of filtering by reviewing the table in the [Education Queensland web filtering website](#).

It is important for families to understand that filtering systems do not replace the need for familial supervision when students are online. Families need to be aware that the child's online activities are the shared responsibility of the family and the student.

Families should also be aware that although a high level of filtering should block a student's access to malicious websites at school and at home, the department cannot guarantee this. If a student downloads software that is designed to modified security settings on the laptop, or change configuration settings on the laptop or software at home, access may be obtained.

- Families, caregivers and students are encouraged to visit the Cybersmart website at <https://www.cyber.gov.au/>
- For further information on the web filtering system visit the QLD government website: <https://www.qld.gov.au/education/schools/procedures/webfiltering>

DEVICE RULES FOR STUDENTS

1. You can use the device for your own educational purposes, both at home and at school. The device may be used for limited personal use but not for commercial purposes (e.g. you cannot use the laptop to earn money).
2. The Department's Acceptable Computer and Internet Use Policy applies to your use of the school computer network and internet when you are using the device. You are reminded of your obligations under that agreement.
3. You must not allow anyone else to use the device for their own purposes, including family members and friends.
4. You must not tell anyone else your MIS Username and Password.
5. You should only use the device at school and at home.
6. If you wish to take the device out of the state, you must seek permission from the school as the device may no longer function due to the protections installed.
7. You accept responsibility for the security and care of the device at all times.
8. You are responsible for backing-up all necessary data. The school is not responsible for any data loss.
9. The software loaded on to the laptop is licensed to the Department of Education or the school. You must ensure that the software is not copied, deleted or transferred, for any reason at all. Unauthorised use may breach copyright laws.
10. While in class, only educational programs are to be used on your device. Games are not to be played. If a student plays a game during class that they have installed on their device or downloaded from the internet, the same school policies and procedures apply to other students with BYOD devices.
11. You must not open, or allow anyone else to open, the hardware case of the device, to install additional hardware (including video card, sound card, network card, modem or disk drive), or to alter the specifications of the device. Commercial repair services excepted.
12. You must take all reasonably necessary steps to prevent a virus from infecting the laptop, including monitoring any data that is downloaded or uploaded onto the device from the Internet or any device and virus checking any USB drives in the laptop.
13. You must ensure that at all times, sufficient space is available on the device, to ensure that school software and other data (eg. digital versions of textbooks), can be installed and functioning correctly. If personal programs have been installed (eg. games), resulting in insufficient space being available on the hard drive of the device for educational software and data to be installed and functioning correctly, then private software must be uninstalled.
14. Images or sound captured by personal technology devices on the school premises or elsewhere, must not be disseminated to others, for the purpose of causing embarrassment to individuals or the school for the purpose of bullying or harassment, or where without such intent a reasonable person would conclude that such outcomes may occur. The school has the right to invoke appropriate disciplinary processes to deal with such behaviour by a student.
15. You must not intentionally use the device or internet services to which it may be connected:
 - a. for any illegal, pornographic, fraudulent or defamatory purposes;
 - b. for bulk transmission of unsolicited electronic mail;
 - c. to send or cause to be sent any computer worms, viruses or other similar programs;
 - d. to menace, bully or harass another person (or use in a way that would be regarded by a reasonable person to be offensive);
 - e. to transmit any harassing, obscene, indecent, offensive, or threatening material or emails;
 - f. to reproduce, distribute, transmit, publish, copy or exploit any material that constitutes an infringement
 - g. of any intellectual property rights (such as copyright) of a third party; or
 - h. in a way that violates any laws, such as privacy laws.
16. The device is to be returned in good condition to the school at the end of the agreement to facilitate transfer ownership to the allocates student. If you cease to be enrolled for any reason before completing the agreement period, you must return the device before leaving the school to facilitate the transfer of ownership.
17. If you do not comply with these rules, there may be disciplinary consequences under our School's Code of Conduct.



Student Equitable Access Device Charter Agreement



Student Name: _____ CARE Class: _____

The Student Equitable Access Device Charter agreement form must be signed and returned to the school before the device is issued.

The student and family/caregiver must carefully read this charter before signing it. Any questions should be addressed to the school and clarification obtained before signing.

In signing below, we acknowledge that we,

accept all policies/guidelines as per the Code of Conduct and Acceptable Use

understand my responsibilities regarding the use of the device and the internet

acknowledge that I understand and agree with all of the conditions detailed in the Charter

understand the difference between accidental damage and carelessness or negligence (see warranty claims and conditions information)

agree to the following provision of an internet filtering level on the device: High (or)

Medium

understand that failure to comply with the Charter could result in recall of the device and/or loss of access for home use

agree to pay the nominal cost of \$300.00 for my child to participate in the Equitable Access Device lease agreement.

After reviewing and understanding the responsibilities outlined in the Acceptable Computer and Internet Use Guidelines and other relevant documents, we agree to the provision of elevated access and web filtering associated with the assignment of the student device.

Student's Name

Student Signature

Date

Family / Caregiver's Name

Family / Caregiver Signature

Date

Designated School Representative Name

School Representative Signature

Date

PLEASE RETURN THIS COMPLETED SHEET TO THE SCHOOL OFFICE WITH PAYMENT



Equitable Access Program Evidence of Financial Hardship Form



Student Name: _____

Parent/Guardian Name: _____

Please provide the following information and documentation to prove financial hardship and be eligible for the Equitable Access Program. All information provided will be kept confidential.

1. Description of Financial Hardship:

Please provide a detailed explanation of the financial hardship your family is currently experiencing. This may include, but is not limited to, the following causes:

- Loss of employment
- Significant unexpected expenses
- Unexpected family emergencies
- Other (specify)

2. Documentation:

Please attach any supporting documentation that you have available to demonstrate your financial hardship. This may include, but is not limited to, the following items:

- Copies of medical bills or invoices
- Proof of unemployment or job termination
- Documentation of any government assistance received (eg Health Care Card)
- Other relevant documents that help support your case

I hereby declare that the information provided above is true to the best of my knowledge and belief, and I understand that providing false information may result in disqualification from the Equitable Access Program:

Family / Caregiver's Name

Family / Caregiver Signature

Date

Please submit this form along with the required supporting documents to the designated school representative when submitting your application.