

CONTENTS

Overview	2
Device	2
Loan Equipment	2
Equipment Ownership	2
Device Care	2
Data Security and Back ups	2
Acceptable Computer and Internet Use	3
Passwords	3
Digital Citizenship	3
Cyber Safety	3
Web Filtering	4
Student's Reporting Requirements	4
Privacy and Confidentiality	4
Intellectual Property and Copyright	5
Misuse and Breaches of Acceptable Usage	5
Damage or Loss of Equipment	
· Theft or Loss	5
· Accidental Damage	
· Wilful and Malicious Damage	
Status Of Laptop Being Issued	5
Software	5
Elevated Access	5
Monitoring and Reporting	6
Period of Participation	6
Laptop Rules For Students	7
Student Laptop Loan Agreement	8

OVERVIEW

This agreement covers the loan of laptop devices to Pimlico State High School students.

The devices are being offered on a loan basis, in order for students to continue accessing curriculum resources while their laptop is being repaired..

The device loaned by the school, is to be used only by the student whose name appears on the Student Loan Agreement Form (last page of this document).

Once the student's own device is repaired, the loan device is expected to be returned to the school in good working condition.

DEVICE

The device that will be provided to students is a Dell 14" laptop, that is suitable for most school based activities that students will be required to complete.

Specific details of the device will be recorded on the Agreement Form, when the student collects the device.

LOAN EQUIPMENT

The equipment referred to in this agreement, consists of a

- Laptop
- Power Charger

Software installed on the laptop includes:

- Microsoft Office 2016 (Word, Excel, PowerPoint, OneNote)

The device will be protected by a current anti-virus program, however for updates to occur, the device must be regularly connected to the school computer network. This can be completed by using the wireless network.

At times, the device may also be required to install software patches (issued by Microsoft or the Department of Education). If this is required, the process is usually performed automatically by the machine, when connected to the school's computer network.

EQUIPMENT OWNERSHIP

All devices are the property of the Queensland Department of Education, Training and Employment.

At the end of the loan period, all devices are to be returned to the school. If the student leaves the school, transfers to a non-government school, moves interstate or overseas, the device must be returned to the school as soon as possible. If the device is not returned, reimbursement will be sought from the parent/care giver. It is also a requirement of using the device, that students provide authorized school staff, access to the device if requested.

DEVICE CARE

The student is responsible for taking care of and securing the device and accessories in accordance with school policy and guidelines. Additional detailed advice for the care of the device can be found on the school web site.

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 and should be completed on an external device, such as external hard drive or USB drive.

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, parental or caregiver permission is sought to give the student access to the internet, based upon the policy contained within Acceptable Use of the Department's Information, Communication and Technology (ICT) Network and Systems.

This policy also forms part of this Student Loan Agreement Form. The acceptable-use conditions apply to the use of the device and internet, both on and off the school grounds.

Communication through internet and online communication services must comply with the Responsible Behaviour Plan For Students, available on the school website.

In adhering to the acceptable use of ICT and Responsible Behaviour Plan, 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 DETE networks
- use the device for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.

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

PASSWORDS

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.

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.

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

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, parent and/or caregiver as soon as is possible.

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.

WEB FILTERING

The Department of Education, Training and Employment (DETE) operates a web filtering system to protect students and restrict access from malicious web activity and inappropriate websites.

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

When students are connected through DETE managed networks, they will have a high level of filtering applied. When students use their devices at home, the filtering system (proxy client), continues to function with a high level of filtering.

It is important for parents to understand that filtering systems do not replace the need for parental supervision when students are online. Parent's need to be aware that the child's online activities are the shared responsibility of the parent and the student.

Parents should also be aware that although a high level of filtering should block a student's access to Facebook 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 tablet or software at home, access may be obtained.

STUDENT'S REPORTING REQUIREMENTS

Students are required to report any internet site accessed that is considered inappropriate, to their teacher.

Any suspected security breach involving students, users from other schools, or from outside the Queensland DETE must also be reported to the school.

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.

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.

DAMAGE OR LOSS OF EQUIPMENT

Laptops are NOT covered by an insurance policy. They are not protected against accidental damage. There is no cover for carelessness, negligence, abuse or malicious damage. Costs incurred by the school for the repair or replacement of devices, may be charged by the school to parents/care givers. In the event of non-compliance of agreed responsibilities, schools may review the student's continued participation in the take home program. Any software or hardware issues, vandalism, damage, loss or theft of the device, must be reported immediately to the school.

Theft and Loss

If the device is stolen outside the school, the parent/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)

Where a device is lost or stolen, the school may invoice a student's parents/care giver, the cost of replacing the device.

Accidental Damage

Where a device is accidentally damaged, the school may invoice a student's parents/care giver, the cost of repairing the device.

Willful and Malicious Damage

Where a school determines that damage had been intentionally caused to a device or a student has disrespected school property, the full cost of repair or replacement may be charged.

STATUS OF LAPTOP BEING ISSUED

The laptop being issued is not new, and has been used by students in the past.

SOFTWARE

The software installed on the device is licensed to the school. The student, parent 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 parent or caregiver may be held liable for any damages incurred.

ELEVATED ACCESS

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

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.

When 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 licence for any software installed and the licence must be appropriate for installation on the device. Devices may be audited by a school requiring students to present a valid software licence for any personal software installed. Devices may be rebuilt at any time for numerous reasons without consultation with students or parents and all local data may be lost in this process.

MONITORING AND REPORTING

Students should be aware that all use of 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, DETE may be required to provide the authorities with access to the device and personal holdings associated with its use.

PERIOD OF PARTICIPATION

The school agrees to provide the laptop to the student from the date soon after all parties sign this agreement and meets arranged payment schedules.

The provision may be ended earlier, at the school's absolute discretion, if:

- the student is no longer enrolled with the school;
- the student is excluded from the school (Note: The laptop may be retained within the school during any period of suspension.)
- in the opinion of the school, the student is not meeting the school's behaviour and educational requirements
- the parent/guardian fails to comply with this Agreement or the School's Acceptable Computer And Internet Use Policy; or
- the student fails to comply with the following Laptop / Tablet Rules for Students or the School's Acceptable Computer And Internet Use Policy.
- school reopens

LOAN DEVICE LOGIN

User name: student

Password: pimlico1!

Laptop 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 School's Acceptable Computer and Internet Use Policy also 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 principal.
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 tablet is licensed to the Department of Education, Training and Employment 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, school staff have the ability to uninstall the game..
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 hard drive specifications of the device.
12. You must not remove the SIM card in the device or place another SIM card in the device, for any reason. The SIM card is a portable memory chip, enabling you to connect to a telecommunication carrier.
13. You must take all reasonably necessary steps to prevent a virus from infecting the tablet, 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.
14. 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.
15. 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.
16. You must not intentionally use the device or internet services to which it may be connected:
 - for any illegal, pornographic, fraudulent or defamatory purposes;
 - for bulk transmission of unsolicited electronic mail;
 - to send or cause to be sent any computer worms, viruses or other similar programs;
 - to menace, bully or harass another person (or use in a way that would be regarded by a reasonable person to be offensive);
 - to transmit any harassing, obscene, indecent, offensive, or threatening material or emails;
 - to reproduce, distribute, transmit, publish, copy or exploit any material that constitutes an infringement of any intellectual property rights (such as copyright) of a third party; or
 - in a way that violates any laws, such as privacy laws.
17. The device is to be returned in good condition to the school at the end of the agreement. If you cease to be enrolled for any reason before completing the agreement period, you must return the device before leaving the school. If the Participation Agreement is ended, you must return the laptop.
18. If you do not comply with these rules, the school will require you to return the device. There may be other disciplinary consequences under our School's Responsible Behaviour Plan for Students.

Student Loan Agreement Form

Student Name: _____ Care Class: _____

Evidence of repair (receipt or note from repairer) indicating expected period of repair, must be attached or sighted.

DEVICE:	
Manufacturer:	
Model:	
Serial #:	
Work Station#:	

The Student Loan Agreement Form must be signed and returned to the school before the device is issued.

The student and parent/care giver must carefully read this agreement before signing it. Any questions should be addressed to the school and clarification obtained before signing.

In signing below, you acknowledge that you,

- accept all policies/guidelines as per the Responsible Behaviour Plan for Students
- understand your responsibilities regarding the use of the device and the internet
- acknowledge that you understand and agree with all of the conditions detailed in the Student Loan Agreement Form
- understand that there may be a cost involved, if the device is lost, stolen or needing repair
- return the loaned device as soon as the school reopens

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 associated with the assignment of the student device.

_____	_____	_____
Student Name	Student Signature	Date
_____	_____	_____
Parent / Caregiver Name	Parent / Caregiver Signature	Date
_____	_____	_____
School Representative Name	School Representative Signature	Date

PLEASE RETURN THIS COMPLETED SHEET TO THE SCHOOL OFFICE