1-to-1 Technology Handbook 2025

Mansfield State High School

Contents

Introduction

This handbook has been developed for families as a guide to the One-to-One Technology Program at Mansfield State High School. The existing Mansfield State High School Laptop Program has been very successful over several years and has brought many benefits to the students. The increased access to computers that the program has allowed has created learning opportunities for students that would not otherwise have been possible. The program was first funded in 2010 by the Federal Government but this funding has now come to an end. The school must therefore look to other ways to provide access to computers for students.

The goal for the future at Mansfield State High School is to provide technology options that are affordable to families while, at the same time, meeting the needs of our students. The school is implementing two models for student use of computers in the classroom: a school-managed laptop program and a home-managed Bring Your Own Device (BYOD) program.

It is inevitable that some families will have difficulty meeting the requirements of the program. The school is committed to ensuring that no student will be disadvantaged because of hardship. The school will make adequate provision for families that can show that they are unable to meet the financial demands of the school managed and BYOD programs.

School contact

Enquiries about Mansfield State High School's laptop program can be directed to:

Michael Sisson
IT Manager

Phone: 07 3452 5333
Email: itsupport@mansfieldshs.eq.edu.au

What is the school managed laptop scheme?

The school managed laptop scheme provides families with a device chosen by the school. The parents/caregivers are required to pay the full cost of device prior to collection. The school purchases and configures the device for the sole use of the student. By the school retaining ownership for the three years of the program, the device is eligible for the school's managed operating system, licensed software and filtering to be installed, as well as to manage any warranty and ADP claims. This arrangement is formalised with all parties (parents/caregivers, students and school) agreeing to a Participation Agreement. During the lifetime of the agreement the school retains ownership of the device, with the option of ownership reverting to the parents/caregivers when the agreement expires and the device is returned to factory state.

School ownership has several benefits, the school can:

- install and maintain the operating system.
- install and maintain antivirus software.
- provide internet filtering at school and at home.
- install and maintain software required for schoolwork (other than software provided in dedicated computer laboratories).
- provide full, secure and reliable student access to the school network and internet.
- provide full technical support through our school IT Service Desk.
- provide access to a hot-swap loan laptop if the device needs repair.
- have 'lemon clause' protection.
- manage all matters relating to device warranty.
- provide an Accidental Damage Protection (ADP) policy.
- manage all matters relating to a claim made under the ADP policy.

At the end of the Participation Agreement the school will dispose of the device according to Department of Education (DoE) policy, with parents/caregivers having the opportunity to take ownership the device. The laptop will be restored to its factory state at this time to remove student restrictions and school-owned software.

All devices will come with a minimum three-year warranty which includes the battery. Devices will all be purchased with Accidental Damage Protection (ADP) warranty and protective bag. Our experience has shown this to be essential for controlling the cost of damage to school devices.

Why does the school retain ownership?

The school retains ownership until the end of the agreement so that we are legally allowed to install school licensed software, including the operating system, as well as to manage any warranty and ADP claims. At the end of the agreement, which is typically three years or the time when the student leaves the school, there is an opportunity to apply to keep the device for no additional fee. If the ownership is transferred before the end of the program there may be the opportunity to transfer the remaining balance of warranty and ADP cover. Transfer of ADP cover may incur an additional fee.

School Managed Laptop costs

The cost of participating in the school managed scheme is determined by the cost of the device. The costs are outlined in the appropriate School Managed Laptop Order Form.

Advantages of the School managed laptop

- All warranty and ADP claims are handled by the school. Note that, as with all insurance, conditions apply.
- Full on-site technical support via the school's IT Help Desk. This includes software rebuilds, network connectivity, printing problems, and troubleshooting of software and hardware problems.
- Access to hot-swap loan devices when device repair is expected to exceed 24 hours.
- Pre-installation and configuration of operating system and antivirus.
- Installation of curriculum specific school software.
- Maintenance of school infrastructure to support student devices.

What is the Bring Your Own Device scheme?

The Bring Your Own Device (BYOD) scheme enables parents/caregivers to purchase from our BYOD portals or another source or to use an existing device, however the device must meet certain minimum requirements. There are technical requirements for the device to connect to the school network. There are also subject specific software requirements. Before buying a device to use at school, families should find out the school's minimum specification of device type, and operating system and software requirements. These specifications relate to the suitability of the device for secure and reliable access to the school network and to meeting student needs in the classroom.

It is a precondition of using the school's network that the device meets the DET security requirements. Up-to-date antivirus software must be in use – we recommend the built in Windows Defender for Windows devices to ensure compatibility. The BYOD device will be able to connect to the school network, student network drives and printer services and access a filtered internet. The school will provide instructions to join the school network via the Microsoft Intune Company Portal which will check the device for compatibility and then manage the device to provide network access. Intune provides the school with information on device specifications, hard drive space and network connectivity. This information is useful when diagnosing connectivity and software installation problems. Because of the wide range of devices, each running their own software configuration, only limited assistance can be provided through the school's ICT Service Desk. Families are responsible for the security, insurance and maintenance of their device.

Comparison of Laptop schemes

	School Managed Laptop	BYOD (Bring your own Device)	
Device	Windows Convertible Laptop	Windows Device	MacBook
Operating system	Windows Education	Windows 11	MacOS Monterey or above
Software Support			
Adobe Creative Cloud	☑	If meeting recommended specifications	Not all applications
Autodesk Applications	☑	If meeting recommended specifications	✕
Other software	All required software supplied by school.	See Subject Device Requirements document	
Hardware Support			
Warranty	Onsite 3 years including battery	Dependant on supplier	
Accidental Damage Protection	3 years ($50 excess)	Dependant on supplier	
Lemon clause	☑	Dependant on supplier	
Fault diagnosis and repair	Provided by onsite technicians	Software support only	
Backup Device	Take home loan device available	Daily loan device available (Cannot be taken home)	
Insurance	School does not provide insurance. We recommending adding the device to your contents insurance policy.		
Internet Filtering			
At school	Internet access provided via school wireless with high level filtering. Use of mobile internet (4G LTE/5G) is not permitted at school.		
At home	Choice of high or medium filtering	Family responsibility	

Software and Applications

School managed laptop students will have ready access to all school software. Subject specific software does change from time to time and school managed laptop students will have access to these changes as required.

The installation and maintenance of software on BYOD devices is the responsibility of the family. Software must be correctly installed to ensure automatic updates. Subject specific software demands do change from time to time. Therefore, a situation may arise where BYOD students will need new software. Details of software to be installed along with any additional costs will be provided with subject book lists.

The School Managed Laptop and BYOD Student Charter

The Student Charter is relevant to all students, regardless of the laptop scheme they are in.

Device care

The student is responsible for taking care of the device in accordance with school policy. Responsibility for loss or damage of a device at home, in transit or at school lies with the student. School managed laptops are covered by Accidental Damage Protection (ADP) but not theft or loss. Families should consider including the device in a home and contents insurance policy. The following precautions should be taken:

- Food or drink should not be placed near the device.
- The device should be carried in a protective case. It should not be carried with the screen open.
- The device must be charged at home and be brought to school with a full charge each day.
- The device should be turned off when not in use, especially when it is carried in its protective case.
- A touch screen only requires a light touch.
- Do not apply pressure to the device lid when it is closed. Avoid placing anything in the carry case that could press against the device lid.
- Avoid putting anything on the keyboard as it can damage the screen when closed.
- Clean the screen with a clean, soft, dry cloth. Do not use a cleaning product.

Data security and back-ups

The student is responsible for the secure backup of all data. It is recommended that students use their school OneDrive account for all schoolwork as this provides redundancy in case of device failure and file history in case of accidental deletion or a file is overwritten. The device should have a virus scanner active to prevent viruses uploaded to OneDrive. We recommend the built in Windows Defender to avoid incompatibility with the school network profile. Students should also be aware that, if repairs need to be carried out on their device, the service agent cannot guarantee the retention of data.

Responsible use

In every Queensland state school, parent/caregiver permission is sought to give each student access to the internet based on the policy in the Education Department’s Information Communication and Technology procedure. This policy also forms part of this Student Charter and applies to the use of the device and the Internet when both at school and not at school. Use of online communication services must also comply with the department’s Code of School Behaviour and the Mansfield State High School Student Code Of Conduct.

While on the school network, students should not:

- try to undermine, hack, or bypass the Department’s hardware and software security mechanisms. This includes disabling settings for virus protection, spam and internet filtering.
- intentionally damage or disable school computers and networks.
- use the school facilities for unauthorised activities, including downloading unauthorised materials.

Students’ use of online communication services may be investigated at the request of appropriate Departmental authorities for the purpose of ensuring compliance with the above.

Passwords

Use of the school's ICT network is secured with a username and password. The password must be difficult enough so as not to be guessed by others and it is to be kept private. It is not to be shared with others. The password should be changed if the student suspects it has become known by someone else. Personal accounts are not to be shared. Students should not allow others to use their personal account for any reason. Students should lock or log off their computer when it is not it use.

Digital citizenship

Interactions online should mirror respectful interpersonal behaviour. Parents/caregivers are requested to ensure that their children understand this responsibility. The school’s Responsible Behaviour Plan outlines school related expectations, guidelines and consequences.

Privacy and confidentiality

Personal accounts are not to be shared. Students should not allow others to use their personal account for any reason. Students should lock or log off their computer whenever it is not it use. Students must not use another person’s school account, including not trespassing in another person's home drive, email or accessing unauthorised school network drives or systems. Additionally, students should not divulge personal information for reasons other than to fulfil the educational requirements of the school. They should ensure that privacy and confidentiality of their own personal information, as well as that of others, is always maintained.

Cybersafety

If a student believes they have received online material that threatens their well-being, they must inform a teacher or parent/caregiver as soon as possible. Students are encouraged to click on the ‘Report cyberbullying’ icon to learn about cybersafety and report concerns. Students must never send or publish offensive, abusive, or discriminatory material, threats or bullying material, or sexual material. Parents/caregivers and students are encouraged to read the Department’s ‘Online awareness: Information for parents and caregivers’.

Web Filtering

To help protect students from malicious activity and unsafe websites, the school operates a web filtering system. Any device connected to the internet through the school network will have filtering applied. This provides a layer of protection against doubtful web sites, spyware and malware, peer-to-peer sessions, scams and identity theft.

This purpose-built web filtering system takes a precautionary approach to blocking websites, including those that do not disclose information about their content. However, despite Departmental efforts to manage internet content when students are at school, illegal, dangerous or offensive information may sometimes be accessible. Teachers exercise their duty of care but avoiding or reducing access to harmful information also requires responsible use by the student. The responsibility is a shared one. The school managed laptops will also be configured for filtering when they are connected to the Internet outside of school. Parents/caregivers choosing the BYOD option are also encouraged to install a filtering system on the device for use when it is connected outside of school. Parents/caregivers are responsible for appropriate internet use by students outside of school. Parents/caregivers and students may visit the Australian Government's iParent website[4] from the Office of the eSafety Commissioner for practical advice to help young people safely use the internet.

Monitoring and reporting

Students should be aware that all use of internet and online communication services can be traced to the account of the user. All material on the device is subject to audit by authorised staff. The school may be required to provide the Queensland Police or Federal Police with access to the device if it is requested.

Breach of responsible use

Students will be held responsible for any actions caused by other persons using their account with the student's knowledge. The school reserves the right to limit access of devices to the intranet, internet, email or other network facilities to ensure the security of the network and to provide a safe environment for all. The misuse of devices may result in disciplinary action which is not limited to the withdrawal of access to school services.

Guidelines

The goal is to ensure the safe and responsible use of services available to students through the provision of clear rules and guidelines. The student must understand that the right to use a device at school is **conditional** on the student abiding by the Charter. The device is primarily provided for an educational purpose. It is not provided for a recreational purpose. Failure to use the device in a responsible way may result in the student losing the device or losing the right to use the school network. When at school the student's use of their device, in or out of class, is determined by a teacher. At all times, the student is obliged to follow a teacher's instructions regarding the student's use of their device. Responsible use requires that the student follows the rules for the use of the device in the Mansfield State High School Handbook.

Intellectual property and copyright

Copying of software and data files may violate copyright laws and may be subject to prosecution.

The student must:

- participate in the 1-to1 Technology Program induction
- Recognise that the device is for education
- look after the device
- practice responsible use and online safety
- protect their password
- regularly back up data
- make sure the device is always fully charged at the start of each school day
- abide by intellectual property and copyright laws
- ensure their login account will not be shared with another student for any reason
- sign the 1-to-1 Technology Program Student Charter

The parents and caregivers must:

- recognise that the purpose of the device is for education
- encourage responsible use and online safety
- provide required software, including antivirus software (BYOD)
- provide a protective case for the device (BYOD)
- sign the 1-to-1 Technology Program Student Charter

References

1. **Department of Education and Training.** Information Security Policy. *Policy and Procedure Register.* [Online] 12 May 2024. https://ppr.qed.qld.gov.au/attachment/information-security-policy.pdf

2. **Mansfield State High School.** Student Code of Conduct [Online] 2024. https://mansfieldshs.eq.edu.au/SupportAndResources/FormsAndDocuments/Documents/Student_code_of_conduct_2024-2026.pdf

3. **Department of Education and Training.** Cybersafety - Students. *Behaviour.* [Online] 2024. https://behaviour.education.qld.gov.au/supporting-student-behaviour/bullying-and-cyberbullying

4. **Office of the esafety Commissioner.** eSafetyparents. [Online] 2024. https://www.esafety.gov.au/parents