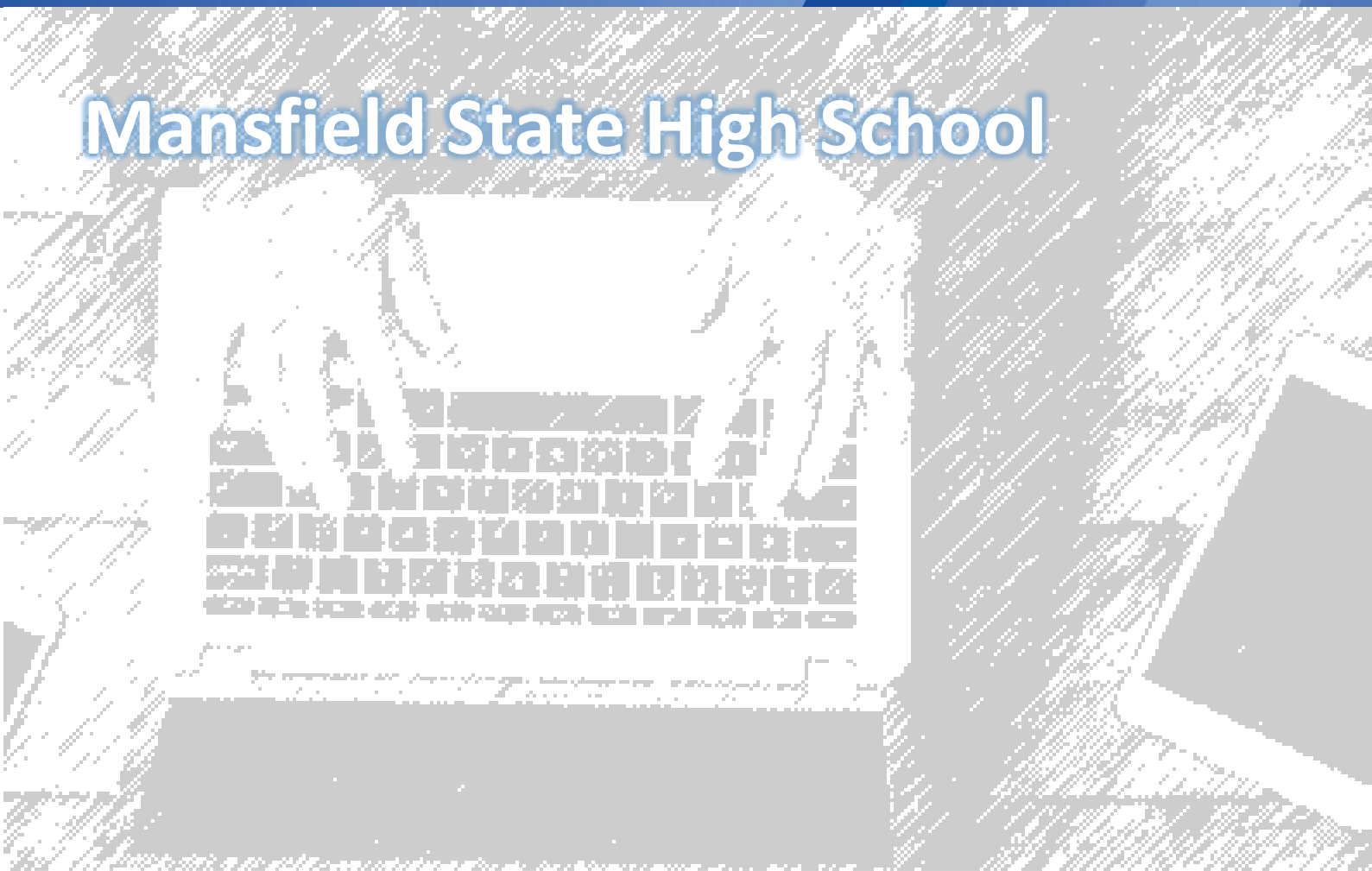
Version 4.0 –2021

Mansfield State High School



Mansfield SHS 1-to-1 Technology Handbook and Charter 2021

School Contacts:

Mark Casey
IT HOD

Michael Sisson
IT Manager

P: 07 3452 5333
E: itsupport@mansfieldshs.eq.edu.au

CONTENTS

INTRODUCTION

This handbook has been developed for parents and students 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 Choose Your Own Device (CYOD) program and a home-managed Bring Your Own Device (BYOD) program.

It is inevitable that some families will have difficulty in joining a 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 CYOD and BYOD programs.

WHAT IS THE CYOD SCHEME?

The Choose Your Own Device (CYOD) scheme provides parents with a device chosen by the school. The parents pay upfront the cost of the device. The school purchases the device for the sole use of the student. By the school **retaining ownership**, we are legally allowed to install school software, including the operating system, as well as to **manage any warranty and ADP claims**. This arrangement is formalised with all parties (parents, 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 when the agreement expires. School ownership has several benefits, the school can:

1. install and maintain the operating system.
2. install and maintain antivirus software.
3. provide internet filtering at school and at home.
4. install and maintain software required for schoolwork (other than software provided in dedicated computer laboratories).
5. provide full, secure and reliable student access to the school network and internet.
6. provide full technical support through our school IT Service Desk.
7. provide access to Hot-Swap laptops if the device needs repair.
8. have CompuTrace anti-theft software installed on the device.
9. have 'lemon clause' protections.
10. manage all matters relating to device warranty.
11. provide an Accidental Damage Protection (ADP) policy.
12. 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 and Training (DET) policy, with parents having the opportunity to apply to keep 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. Transfer of ownership may include transfer of any remaining warranty and ADP coverage.

CYOD COSTS

The cost of participating in the CYOD scheme is mostly determined by the cost of the device. The costs are outlined in the appropriate *CYOD Order Form*. Part of the school levy is also used to fund support for the program.

ADVANTAGES OF THE CYOD SERVICE GUARANTEE FEE

- All warranty and ADP claims are handled by the school. Note that, as with all insurance, conditions apply. A summary of terms can be found in the Selection Guide.
- Full on-site technical support via the school's ICT Service Desk. This includes software rebuilds, network connectivity, printing problems, and troubleshooting of software and hardware problems.
- Access to Hot-Swap devices when device repair is expected to exceed 24 hours.
- Pre-installation of generic software 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 allows parents 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 BYOD device to connect to the school network. There are also subject specific software requirements. Part of the school levy contributes to the running of the program which includes:

1. BYOD Wi-Fi device connection subscription fee.
2. School infrastructure requirements to support the BYOD scheme.
3. Software license fees for BYOD devices.
4. Technical support to connect to the school Wi-Fi and printers, and to install some software.
5. Basic fault diagnosis, problem solving and recommendations for action.

Before buying a device to use at school parents and students 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.

That the device meets the DET's security requirements is a precondition to use of the school's network. Up-to-date antivirus software must be in use. 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 install client software to allow device visibility and management while the device is connected to the school network. This will allow students to install software, use a self-help service and submit support requests to the school's ICT Service Desk. The client software 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 minimal assistance can be provided through the school's ICT Service Desk. Students and parents are responsible for the security, insurance and maintenance of their device.

COMPARISON OF CYOD AND BYOD SCHEMES

	CYOD (Choose Your Own device)	BYOD (Bring your own Device)	
Device	School purchased device	Home supplied Windows device (must meet minimum specification)	Home supplied Mac device (must meet minimum specification)
Operating system	Windows 10 Education Version	Windows 10	MacOS 10.12 (Sierra) or above
Adobe Creative Cloud	✓	If meeting recommended specifications	Not all applications
Autodesk Applications	✓	If meeting recommended specifications	×
School software (As per subject selection)	All required software supplied by school.	See below.	
Lemon clause	✓	Dependant on supplier	
CompuTrace anti-theft protection	✓	Not generally provided for personal computers	
Network access	✓	Requires approved antivirus software and dual band wireless	
Internet access	✓	Non-filtered access is forbidden by EQ; only school provided internet is allowed at school.	
Internet Filtering			
At school	High level filtering		
At home	Family's choice of high or medium filtering	Responsibility of the family	
Onsite Technical Support			
Warranty (including battery)	3 years (Next business day)	Responsibility of the family	
Accidental damage protection (ADP)	3 years	Responsibility of the family	
Operating system rebuilds	✓	Responsibility of the family	
Fault diagnosis and remedy	✓	Limited onsite warranty support available on BYOD portal devices	

SOFTWARE AND APPLICATIONS

CYOD students will have ready access to all school software. Subject specific software does change from time to time and CYOD 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 CYOD AND BYOD STUDENT CHARTER

The Student Charter is relevant to all students, regardless of the CYOD or BYOD 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. CYOD devices are covered by Accidental Damage Protection (ADP) and the school's insurance against theft and loss. BYOD parents should consider including the BYOD 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 should be charged overnight. It should come to school fully charged 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.
- 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. While at school students can save data on the school network. All files must be scanned using antivirus software before being placed on the school network. Students can save data on their own device for use out of school. The backup of this data is the responsibility of the student and it should be done on an external device. 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 parental 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 (1). 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 (2) and the Mansfield State High School Responsible Behaviour Plan (3).

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 are requested to ensure that their children understand this responsibility. The school's Responsible Behaviour Plan outlines school related expectations, guidelines and consequences.

CYBERSAFETY

If a student believes they have received online material that threatens their well-being, they must inform a teacher or parent as soon as possible. Students are encouraged to click on the 'Report cyberbullying' icon to learn about cybersafety and report concerns (4). 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' (5).

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 accessed. 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 CYOD devices will also be configured for filtering when they are connected to the Internet outside of school. Parents 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 are responsible for appropriate internet use by students outside of school. Parents, caregivers and students may visit the Australian Government's iParent website (6) from the Office of the eSafety Commissioner for practical advice to help young people safely use the internet.

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.

INTELLECTUAL PROPERTY AND COPYRIGHT

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

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.

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 Communication and Technology. *Policy and Procedure Register.* [Online] 9 May 2017. http://ppr.det.qld.gov.au/corp/ict/management/Pages/Information-Communication-and-Technology-(ICT).aspx.

2. —. Code of School Behaviour. *Behaviour.* [Online] 2006. http://education.qld.gov.au/behaviour/docs/code-school-behaviour-a4.pdf.

3. **Mansfield State High School.** Rules and Policies. *Mansfield State High School.* [Online] 2017. https://mansfieldshs.eq.edu.au/Supportandresources/Formsanddocuments/Documents/Responsible%20Behaviour%20Plan.pdf

4. **Department of Education and Training.** Cybersafety - Students. *Behaviour.* [Online] 2017. http://behaviour.education.qld.gov.au/cybersafety/Pages/students.aspx

5. —. Cybersafety - Parents. *Behaviour.* [Online] 2017. http://behaviour.education.qld.gov.au/cybersafety/Pages/parents.aspx

6. **Office of the esafety Commissioner.** iParent. *eSafety.* [Online] 2017. https://esafety.gov.au/education-resources/iparent