

BYOD PARTICIPATION AGREEMENT 2021



TERMS OF PARTICIPATION

Although it is preferable for students to join the Mansfield Laptop Program, we understand that this is not suitable for all families. For this reason, Mansfield SHS will allow students to bring their own device. This is known as the BYOD program. There are several considerations for families wanting to “BYOD” which will be outlined in this document.

1. PERIOD OF PARTICIPATION

- 1.1 The period of participation is the current school year. Families will need to sign a new agreement each year.
- 1.2 The School agrees to provide access to the school network through a mobile device management system.

2. FEE FOR PARTICIPATION

- 2.1 Fees for the BYO Program are incorporated in the school levy. There is no extra payment for BYOD.
- 2.2 If the school levy is not paid then access to the school network may be reviewed.

3. MINIMUM SPECIFICATIONS

- 3.1 All Devices must meet Mansfield’s BYOD Minimum Requirements; devices that do not meet the requirements will not be connected to the school’s resources. Some subjects may require the recommended specifications – see Subject Requirements document for more information.

Minimum Device Specifications

Platform	Windows Laptop or 2-in-1, MacBook (No Phones, Android Tablets or Chromebooks)
Screen Size	11”+ Screen
Processor	Intel Pentium or AMD Athlon (Windows ARM devices are not supported)
Memory	4GB
Operating System	Windows 10 or Mac OS High Sierra+
Wireless	Must be 5GHz capable
Battery Life	8+ hours

Recommended Device Specifications

Platform	Windows Laptop or 2-in-1
Screen Size	13”+ Touchscreen
Processor	Intel Core i3+ or AMD Ryzen3+
Memory	8GB+
Operating System	Windows 10
Wireless	Must be 5GHz capable
Battery Life	8+ hours

Minimum Software requirements

Antivirus	Up-to-date version of trusted antivirus software suite
PDF Viewer	e.g. Adobe Acrobat Reader
Office Suite	e.g. Microsoft Office (available for free to Qld school students)
Internet Browser	e.g. Google Chrome, Mozilla Firefox

4. CONNECTION TO THE INTERNET

- 4.1 The school provides secured, filtered access to the Internet via its high speed wireless network. Student access to the Internet is governed by the School’s ICT Policy and Responsible Behaviour Plan.
- 4.2 The school uses the 5GHz wireless band as it provides a more stable connection and less interference. All BYO Devices must be capable of connecting to a 5GHz Wireless Network, the school will be unable to connect devices that do not support 5GHz. If you are unsure consult the manufacturer’s website. (Some lower cost laptops do not support 5GHz Wireless.)
- 4.3 The school provides access to the school network via a mobile device management system (MDM). Enrolment in the system is best completed at home after attending school for the first time. All students are required to have Administrative Access to their BYO device to allow connection and installation of school resources.
- 4.4 The school reminds the parent/guardian of their obligations under this agreement. 3/4G ability e.g. USB Dongles, should be disabled or not brought to school as this function when activated allows students to bypass the EQ internet security filters.

BYOD PARTICIPATION AGREEMENT 2021



The school will take no responsibility for the content accessed by students using 3/4G facility on their personally owned devices.

4.5 At school, the carriage service and connectivity to the internet is governed by the School's Student Network/Internet Access Agreement and the School's Internet Usage Policy

4.6 When students use their devices at home the filtering is the responsibility of the family. Please note that some filtering solutions may interfere with network access at school. Care should be taken when selecting a filtering product to ensure school access can be maintained.

5. IMPROPER USE

5.1 The parent/guardian must ensure that the laptop is not tampered with in order to connect to internet services outside the school and that the laptop is not used:

- 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 or harass another person (or used 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.

6. SOFTWARE

6.1 Only licensed software authorised by the School can be stored or otherwise loaded on to the laptop. The parent/guardian must ensure that any other software is not loaded onto the laptop.

6.2 The software loaded on the laptop is licensed to the Department of Education and Training or the School. The parent/guardian must ensure that the software is not copied, deleted or transferred, for any reason at all, without prior written consent from the School. Unauthorised use may breach copyright laws and the parent/guardian may be held liable for any damages incurred.

7. VIRUS PROTECTION

7.1 Viruses have the potential to severely damage and disrupt operations within the School and the Department's network. They can also be costly to restore the network, infected hardware or software to its previous state and operability.

7.2 Viruses can enter laptop computers through: removable media such as CDs, DVDs, floppy disks and USB memory sticks
Emails/Phishing attempts (emails linking to malicious websites)
The internet (including web browsing, FTP programs and chat rooms)
file download
Network file shares, such as servers and shared folders.

7.3 Students have the right to use their laptops at home for personal use. If accessing the Internet from home via cable or wireless, they should take all steps to protect the school-owned laptop and the department's computer network from virus attacks.

7.4 The parent/guardian must take reasonably necessary steps to prevent a virus from infecting the laptop, including monitoring

- Any data that is uploaded onto the Laptop from any device.
- Virus checking any USB drives in the Laptop.

8. REPAIR AND MAINTENANCE

8.1 All maintenance for the BYO laptop, operating system, software and/or apps purchased by the family are the responsibility of the family. Families should ensure quick maintenance turnaround for student devices.

8.2 A limited number of Loan laptops may be available from the IT office for use while repairs are occurring; these will only be available for use at school. The school provides minimal IT Support for BYO Devices.

8.3 If you run into a problem, students are advised to see the Mansfield IT staff who will attempt to diagnose the fault. If the problem is not able to be resolved by IT Staff, they may recommend a course of action for repair (e.g. Re-install windows, warranty claim, insurance claim etc.)

9. LOSS OR DAMAGE

9.1 It is recommended that your device is covered by an extended warranty, statistically a computer will require, on average, 2.5 repairs during its 3-year life cycle.

9.2 Students are responsible for ensuring laptops are secure at all times, it is recommended that students do not leave their devices unattended in public places. The school is not responsible for any damage to student devices and will not be accountable for any lost or stolen student devices or property.

9.3 When purchasing your laptop please look at options to purchase accidental damage protection for your IT device. ADP covers your device with accidental damage on and off the school campus. Fire, theft and acts of God are usually not covered under these programs and we request you to include it in your personal or home insurance. The insurance can be purchased with your computer vendor or any insurance company. All insurance claims must be settled between you and

the insurance company. Statistically, 60% of repairs at the school are considered non-warranty. E.g. repairing a cracked screen from a drop. Purchasing insurance for your BYOD is a personal choice.

LAPTOP RULES FOR STUDENTS

1. The Laptop must be used for educational purposes while at school.
2. If you do not comply with these Laptop Rules for Students, you are not allowed to connect the laptop to the network. There may be other disciplinary consequences under your School's Responsible Behaviour Plan and the School's Student ICT Network Access Agreement and Usage Agreement also apply to your use of the network / internet when you are accessing the internet using the laptop. You are reminded of your obligations under that agreement and policy.
3. You accept responsibility for the security and care of the laptop. You must not tell anyone else your account password.
4. You are responsible for backing-up all necessary data. The School is not responsible for any data loss. Therefore, please ensure all your school work and important documents are backed up onto external storage devices or OneDrive.
5. You must take all reasonable steps to prevent a virus from infecting the laptop, including monitoring any data that is downloaded or uploaded onto the laptop from the Internet or any device and virus checking any USB drives in the laptop.
6. When not in use, the laptop must be stored in a carry case and either kept in your possession or in a secure place.
7. Images or sound captured by personal technology devices on the school premises or elsewhere must not be disseminated to others using the laptop, 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.
 - You must not intentionally use the laptop 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 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.
8. In particular you must not use the laptop (or any internet services to which it may be connected) to bully, harass or be unkind to other persons.

USE AND CARE OF THE LAPTOP COMPUTER

USAGE

- Don't use technology devices on soft surfaces (e.g. sofa, bed or carpet) because it can restrict airflow and cause overheating.
- Avoid dropping or bumping technology devices.
- Don't place technology devices in areas that may get very hot.
- Don't get technology devices wet, even though they will dry and appear to operate normally, the circuitry could slowly corrode and pose a safety hazard.
- Follow all instructions given by staff.
- Login correctly and logoff when finished.
- Always shut down computers through the 'Start – Shutdown' mechanism.
- Always package, carry and store technology devices in appropriate and secure carry cases for transporting.
- Personalise technology devices with methods approved by the school, to ensure students do not get the devices mixed-up.
- Don't place objects on top of your laptop and never carry it around while it is turned on.
- Avoid exposing your laptop computer to direct sunlight or sources of heat such as desk lamps; dust, dirt, rain, liquids or moisture; heavy shock or vibration

HANDLING YOUR LAPTOP COMPUTER

- Try to avoid moving your laptop around when it is on. Before switching on, gently place your laptop on a stable surface and then switch on.
- You need to be careful with your laptop while it is in the bag. Do not drop the bag from your shoulder. Always place the laptop bag gently down.
- Be careful when putting the laptop in the car that no other items are on top of it and nothing will roll onto the laptop bag.
- Laptops should be switched off or hibernated before being placed into the bag.
- The bag should be fully zipped up before being carried

BYOD PARTICIPATION AGREEMENT 2021



- The bag should be fully unzipped before removing the laptop to avoid non-warranty bag damage. Packing away your laptop computer
- Always store your laptop bottom down and with the LCD facing away from the front of the backpack.
- Do not wrap the cord too tightly around the power adapter or the cord will become damaged.

LCD SCREEN

- LCD screens are delicate - they don't like being poked, prodded, pushed or slammed. Never pick up your laptop by its screen. Don't slam the screen closed and always be gentle when putting your laptop down.
- To clean your LCD screen:
- Switch off your laptop computer.
- Lightly dampen a non-abrasive cloth with water and gently wipe screen in a circular motion.
- Do not directly apply water or cleaner to the screen.
- Avoid applying pressure to the screen.

AC ADAPTER

- Connect your adapter only to your laptop computer.
- Do not step on your power cord or place heavy objects on top of it. Keep your cord away from heavy traffic areas.
- When unplugging the power cord, pull on the plug itself, rather than the cord.
- Do not wrap your cord tightly around the adapter box.

KEYBOARD

- Gently brush your keyboard with a clean soft bristled paint brush or similar to remove dirt.
- If any key tops are missing or keys are in a damaged state, take your laptop to the IT department to be repaired immediately. A single key top can easily be replaced but continuing to use the keyboard with a missing key top can result in having to replace the entire keyboard which will be treated as a non-warranty claim.

CASE CLEANING

- Wipe with a dampened non-abrasive cloth. Do not spray any cleaners directly on to the casing.
- Gently rub your laptop casing with the moistened cloth to remove any dirty marks.

SECURITY

- Report any technology device fault or suspected virus activity to the nearest staff member.
- Undertake virus scans of computers after home usage and prior to reconnecting to the school's ICT network.
- Make regular backups of your saved work.
- Keep your login and password confidential.
- Don't tamper either physically or electronically with either hardware or software settings.
- Don't attempt or undertake any malicious behaviour towards the School's ICT resources.
- Don't attempt to make unauthorised access to ICT resources or entities.
- Don't have food or drink near the technology device.
- A good idea is to attach a fairly large name tag in a bright colour to the case or bag so it is easy to identify. Remember, over the life of the program this laptop may not be with the same student the whole time, and it may need to be returned for servicing at any time.

SOFTWARE

- Don't copy any software from the School's ICT network or system.
- All technology equipment should only have operating systems loaded that are compliant with departmental standards.
- Keep your virus check software up-to-date. If your virus check software detects virus activity then carefully follow the instructions for removal and advise the nearest staff member. If unsure, quarantine your computer and disks and immediately consult with the IT staff.
- Always adhere to licensing and copying agreements.
- Never use technology devices to engage in illegal activity, including violation of copyright or other contracts.

BATTERIES

- Don't use incompatible computer batteries and chargers.
- Computer batteries can get hot during use. Do not use your computer on your lap.
- Have fully charged battery/batteries at the start of each school day. All charging should be undertaken at home, as the school will not have the infrastructure or resources available to charge batteries for every student.
- Don't permit a loose battery to come in contact with metal objects, such as coins, keys or jewellery.

BYOD PARTICIPATION AGREEMENT 2021



- Don't crush, puncture or put a high degree of pressure on the battery as this can cause an internal short-circuit, resulting in overheating.
- Don't get your battery wet, even though it will dry and appear to operate normally, the circuitry could slowly corrode and pose a safety hazard.
- Follow battery usage, storage and charging guidelines found in the computer's user guide.

WET WEATHER

- Particular care needs to be taken during wet weather, whether at school or while travelling to/from school or at home
- Never drop your bag into a puddle, leave it out in the rain or where water might run, or have it otherwise unprotected from rain – if your school bag gets wet, your laptop might also.

TECHNICAL SUPPORT

- Students can access the School's IT Department before school, during lunch times and after school to log a fault with their laptop or seek technical advice from the School's technicians.