# Laidley State High School

# Digital Futures Guidebook

Version 6, 2021

# Contents

# Laidley State High School – Digital Futures

This document outlines the requirements for devices, responsibilities of students with devices at school, tips for care and safe use of devices.

Over the last decade teaching and learning has continued to move towards a digital platform allowing teachers and students to connect beyond the classroom. Laidley SHS believes that it is important to learn valuable knowledge and also the skills to help them succeed in the future.

In order for this to occur effectively and equitably Laidley SHS has provided three possible pathways to enable students to be part of our Digital Futures.

1. BYOD (Bring Your Own device)
2. Laidley SHS Laptop Hire Scheme
3. Laidley SHS EQUITY Scheme

## BYOD Program

Bring Your Own '*Device*' (BYOD) is a new pathway supporting the delivery of 21st century learning. It is a term used to describe a digital device ownership model where students or staff use their personally-owned mobile devices to access the department's information and communication (ICT) network.

Access to the department's ICT network is provided only if the mobile device meets the department's security requirements which, at a minimum, requires that anti-virus software has been installed, is running and is kept updated on the device Advice for State Schools on Acceptable use of ICT Facilities and Devices.

Students are responsible for the security, integrity, insurance and maintenance of their personal mobile devices and their private network accounts.

The BYOD acronym used by the department refers to the teaching and learning environment in Queensland state schools where personally-owned mobile devices are used. The '*Device*' in BYOD represents more than a personally-owned mobile device; it also includes software, applications, connectivity or carriage service.

The department has carried out extensive BYOD research within Queensland state schools. The research has built on and acknowledged the distance travelled in implementing 1-to-1 computer to student ratio classes across the state, and other major technology rollouts.

We have chosen to support the implementation of a BYOD model because:

- BYOD recognises the demand for seamless movement between school, work, home and play
- Our BYOD program assists students to improve their learning outcomes in a contemporary educational setting
- Assisting students to become responsible digital citizens enhances the teaching learning process and achievement of student outcomes as well as the skills and experiences that will prepare them for their future studies and careers.

## Device selection

Before acquiring a device to use at school the parent or caregiver and student should be aware of the school's specification of appropriate device type, operating system requirements and software. These specifications relate to the suitability of the device to enabling class activities, meeting student needs and promoting safe and secure access to the department's network.

***Minimum Hardware Requirements for device selection***

In order for effective teaching and learning to take place, the device selected by parents must meet the following minimum standards for learning:

- 4 Gb ram (8 Gb recommended)
- Internal hard drive (64 Gb minimum with 128 Gb or greater recommended)
- USB port
- Operating systems

  - Windows 10
  - Apple OS X 10.6+

- Minimum Screen size of 11.6 inch
- Wi-Fi connectivity (802.11n - minimum with 802.11ac – recommended)
- Microsoft office and Adobe software is available through the school so does not need to be included
- Battery – 6 hours working life without need for recharging
- Insurance (replacement insurance recommended)
- Carry cases for protection

NOTE: ChromeBooks/Android devices are **not supported**.

The school's BYOD program includes access to printing, filtered internet access, and file access and storage through the department's network while at school and limited Technical Support. However, the school's BYOD program does not include hands-on school technical support or charging of devices at school. Our technical support team may provide limited diagnostic advice that may be reported back to the vendor, however they will not be conducting any hardware repairs or software installation.

**Special Note: Windows 10 comes with "Windows Defender" built-in.**
Therefore, if you are purchasing a laptop with Windows 10 on it, you *do not require a separate Anti-Virus program.*

# Laidley SHS Laptop Hire Program

As well as supporting students and families to be part of the BYOD pathway, there is also the ability for students to hire one of the school owned laptops. This allows families to utilise the device 24/7 in the classroom and at home to engage students with digital learning but at a reduced cost. The device is able to connect to the school's network for internet access with content filtering, network storage and printing services. While at home the device is able to be connected to the home network where it can access personal networks, internet and printing devices.

While the device is hired to the student it is important to understand that it is their responsibility and as such, any damages incurred will result in the student being invoiced for the cost of repairs.

In order for students to be part of the Laidley SHS Laptop Hire Program families must fill in and return the **Digital Futures Pathway and Responsible Use Agreement form** (located at the back of this document) along with payment of the Hire Fee. Once the form and payment have been received, the school will prepare the next available device and notify the student through the morning notices when it is ready for collection.

## Laidley SHS EQUITY Program

The Laidley SHS EQUITY Program allows families who may be experiencing financial difficulties the ability to work with the school to provide devices for their student/s. The EQUITY Program provides students to the same device and access as the Laidley SHS Laptop Hire Program but at a reduced cost.

In order to be considered for the EQUITY Program, families will be required to fill in an EQUITY Program form along with the **Digital Futures Pathway and Responsible Use Agreement form** (located at the back of this document). Please submit both forms to the school administration along with supporting documentation to enable the School's BYOD team make a decision regarding the application. Once a decision has been made, the school will contact families to notify them of the decision.

It is important to note, that while a device is hired to a student, that it is their responsibility and as such, any damages incurred will result in the students being invoiced the cost of repairs.

## Device care

The student is responsible for taking care of and securing the device and accessories in accordance with school policy and guidelines. Responsibility for loss or damage of a device at home, in transit or at school belongs to the student. Advice should be sought from your insurance company regarding inclusion on your home and contents insurance policy.

It is advised that accidental damage and warranty policies are discussed at the point of purchase to minimise the financial impact and disruption to learning should a device not be operational.

School lockers will be available for hire to provide a safe and secure location to store devices during times that the device is not in use.

## General precautions

- Food or drink should never be placed near the device.
- Plugs, cords and cables should be inserted and removed carefully.
- Devices should be carried within their protective case where appropriate.
- Carrying devices with the screen open should be avoided.
- Ensure the battery is fully charged each day.
- Turn the device off before placing it in its bag.

## Protecting the screen

- Avoid poking at the screen — even a touch screen only requires a light touch.
- Don’t place pressure on the lid of the device when it is closed.
- Avoid placing anything on the keyboard before closing the lid.
- Avoid placing anything in the carry case that could press against the cover.
- Only clean the screen with a clean, soft, dry cloth or an anti-static cloth.
- Don’t clean the screen with a household cleaning product.

## Data security and back-ups

Students must ensure they have a process of backing up data securely. Otherwise, should a hardware or software fault occur, assignments and the products of other class activities may be lost.

The student is responsible for the backup of all data. While at school, students are required to save data to the school’s network (H drive), which is safeguarded by a scheduled backup solution. All files must be scanned using appropriate anti-virus software before being downloaded to the department's ICT network.

Students are also able to save data locally to their device for use away from the school network. The backup of this data is the responsibility of the student and should be backed-up on an external device, such as an external hard drive or USB drive.

Students should also be aware that, in the event that any repairs need to be carried out the service agents may not guarantee the security or retention of the data. For example, the contents of the device may be deleted and the storage media reformatted.

# Acceptable personal mobile device use

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

This policy also forms part of this Student Laptop Charter. 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 also comply with the department's Code of School Behaviour and the Responsible Behaviour Plan available on the school website.

While on the school network, 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, school or government networks
- Use the device for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.

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

## Passwords

Use of the school's ICT network is secured with a user name and password. The password must be difficult enough so as not to be guessed by other users and is to be kept private by the student and not divulged to other individuals (e.g. a student should not share their username and password with fellow students).

The password should be changed regularly, as well as when prompted by the department or when known by another user.

Personal accounts are not to 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.

Students should also set a password for access to their BYOD device and keep it private.

Parents/caregivers may also choose to maintain a password on a personally-owned device for access to the device in the event their student forgets their password or if access is required for technical support. Some devices may support the use of parental controls with such use being the responsibility of the parent/caregiver.

## 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 are easily searchable and accessible. This content may form a permanent online record into thefuture.

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

Parents are requested to ensure that their child understands this responsibility and expectation. The school's Responsible Behaviour Plan also supports students by providing school related expectations, guidelines and consequences.

## 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 or caregiver as soon as is possible.

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

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

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.

Parents, caregivers and students are encouraged to read the department's Cybersafety and Cyberbullying guide for parents and caregivers.

## Web filtering

The internet has become a powerful tool for teaching and learning, however students need to be careful and vigilant regarding some web content. At all times students, while using ICT facilities and devices, will be required to act in line with the requirements of the *Code of School Behaviour*) and any specific rules of the school. To help protect students (and staff) from malicious web activity and inappropriate websites, the school operates a comprehensive web filtering system. Any device connected to the internet through the school network will have filtering applied.

The filtering system provides a layer of protection to staff and students against:

- inappropriate web pages
- spyware and malware
- peer-to-peer sessions
- Scams and identity theft.

This purpose-built web filtering solution takes a precautionary approach to blocking websites including those that do not disclose information about their purpose and content. The school's filtering approach represents global best-practice in internet protection measures. However, despite internal departmental controls to manage content on the internet, illegal, dangerous or offensive information may be accessed or accidentally displayed. Teachers will always exercise their duty of care, but avoiding or reducing access to harmful information also requires responsible use by the student.

Students are required to report any internet site accessed that is considered inappropriate. Any suspected security breach involving students, users from other schools, or from outside the Queensland DET network must also be reported to the school.

The personally-owned devices have access to home and other out of school internet services and those services may not include any internet filtering. Parents and caregivers are encouraged to install a local filtering application on the student's device for when they are connected in locations other than school. Parents/caregivers are responsible for appropriate internet use by students outside the school.

Parents, caregivers and students are also encouraged to visit the eSafety website for resources and practical advice to help young people safely enjoy the online world.

## Privacy and confidentiality

Students must not use another student or staff member's username or password to access the school network or another student's device, including not trespassing in another person's files, home drive, email or accessing unauthorised network drives or systems.

Additionally, students should not divulge personal information via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school. 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. Students should also not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. They should ensure that privacy and confidentiality is always maintained.

# Intellectual property and copyright

Students should never plagiarise information and should observe appropriate copyright clearance, including acknowledging the original author or source of any information, images, audio etc. 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.

Copying of software, information, graphics or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.

## Software

Some software, such as Microsoft Office and Adobe, are available free of charge through the school. Instructions to download this software is available on the school website.

The school may also recommend other software applications in order to meet the curriculum needs of particular subjects. Parents/caregivers may be required to install and support the appropriate use of the software in accordance with guidelines provided by the school. This includes the understanding that software may need to be removed from the device upon the cancellation of student enrolment, transfer or graduation.

## 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, the school may be required to provide the authorities with access to the device and personal holdings associated with its 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 school reserves the right to restrict/remove access of personally owned mobile devices to the intranet, internet, email or other network facilities to ensure the integrity and security of the network and to provide a safe working and learning environment for all network users. The misuse of personally owned mobile devices may result in disciplinary action which includes, but is not limited to, the withdrawal of access to school supplied services.

# Responsible use of Laidley SHS Technology

Our goal is to ensure the safe and responsible use of facilities, services and resources available to students through the provision of clear guidelines.

**Responsibilities of stakeholders involved in the Digital Futures program:**

***School***

- BYOD program induction — including information on (but not responsible for) connection, care of device at school, workplace health and safety, appropriate digital citizenship and cybersafety
- network connection at school
- internet filtering (when connected via the school's computer network)
- some technical support (please consult Technical support table below)
- some school-supplied software e.g. Adobe, Microsoft Office 365 …
- printing facilities
- school representative signing of Digital Futures Pathway Agreement.

***Students***

- read the Digital Futures program induction information
- acknowledgement that core purpose of device at school is for educational purposes
- care of device
- appropriate digital citizenship and online safety (for more details, see here)
- security and password protection — password must be difficult enough so as not to be guessed by other users and is to be kept private by the student and not divulged to other individuals (e.g. a student should not share their username and password with fellow students)
- some technical support (please consult Technical support table below)
- maintaining a current back-up of data
- charging of device before arriving at school
- abiding by intellectual property and copyright laws (including software/media piracy)
- internet filtering (when not connected to the school's network)
- ensuring personal login account will not be shared with another student, and device will not be shared with another student for any reason
- students can hire school lockers to store their device securely on occasions when the device is not being used.
- understanding and signing the Digital Futures Pathway and Responsible Use Agreement.

***Parents and caregivers***

- read the Digital Futures program induction information
- acknowledgement that core purpose of device at school is for educational purposes
- internet filtering (when not connected to the school's network)
- encourage and support appropriate digital citizenship and cybersafety with students (for more details, see here)
- some technical support (please consult Technical support table below)
- required software, including sufficient anti-virus software
- protective case for the device
- adequate warranty and insurance of the device
- understanding and signing the BYOD Charter Agreement.

## Technical support

| | Connection: | Hardware: | Software: |
|---|---|---|---|
| **Parents and Caregivers** | ✓ (home-provided internet connection) | ✓ | ✓ |
| **Students** | ✓ | ✓ | ✓ |
| **School** | ✓ school provided internet connection | (dependent on school-based hardware arrangements with selected vendors) | ✓ (some school-based software arrangements) |
| **Device vendor** | | ✓ (see specifics of warranty on purchase) | |

**The following are examples of responsible use of devices by students:**

- Use mobile devices for:
  - engagement in class work and assignments set by teachers
  - developing appropriate 21st Century knowledge, skills and behaviours
  - authoring text, artwork, audio and visual material for publication on the Intranet or Internet for educational purposes as supervised and approved by school staff
  - conducting general research for school activities and projects
  - communicating or collaborating with other students, teachers, parents, caregivers or experts as part of assigned school work
  - accessing online references such as dictionaries, encyclopaedias, etc.
  - researching and learning through the school's eLearning environment
  - ensuring the device is fully charged before bringing it to school to enable continuity of learning.
- Be courteous, considerate and respectful of others when using a mobile device.
- Switch off and place out of sight the mobile device during classes, where these devices are not being used in a teacher directed activity to enhance learning.
- Use the personal mobile device for appropriate private use before or after school, or during lunch breaks.
- Seek teacher's approval where they wish to use a mobile device under special circumstances.

**The following are examples of irresponsible use of devices by students:**

- using the device in an unlawful manner
- creating, participating in or circulating content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- disabling settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard
- downloading (or using unauthorised software for), distributing or publishing of offensive messages or pictures
- using obscene, inflammatory, racist, discriminatory or derogatory language

- using language and/or threats of violence that may amount to bullying and/or harassment, or even stalking
- insulting, harassing or attacking others or using obscene or abusive language
- deliberately wasting printing and Internet resources
- intentionally damaging any devices, accessories, peripherals, printers or network equipment
- committing plagiarism or violate copyright laws
- using unsupervised internet chat
- sending chain letters or spam email (junk mail)
- accessing private 3G/4G networks during lesson time
- knowingly downloading viruses or any other programs capable of breaching the department's network security
- using the mobile device's camera anywhere a normal camera would be considered inappropriate, such as in change rooms or toilets
- invading someone's privacy by recording personal conversations or daily activities and/or the further distribution (e.g. forwarding, texting, uploading, Bluetooth use etc.) of such material
- using the mobile device (including those with Bluetooth functionality) to cheat during exams or assessments
- take into or use mobile devices at exams or during class assessment unless expressly permitted by school staff.
- Playing games or watching videos in class unless directed to do so by a teacher as part of a learning activity

**In addition to this:**

Information sent from our school network contributes to the community perception of the school. All students using our ICT facilities are encouraged to conduct themselves as positive ambassadors for our school.

- Students using the system must not at any time attempt to access other computer systems, accounts or unauthorised network drives or files or to access other people's devices without their permission and without them present.

- Students must not record, photograph or film any students or school personnel without the express permission of the individual/s concerned and the supervising teacher.

- Students must get permission before copying files from another user. Copying files or passwords belonging to another user without their express permission may constitute plagiarism and/or theft.

- Students need to understand copying of software, information, graphics, or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.

- Parents and caregivers need to be aware that damage to mobile devices owned by other students or staff may result in significant consequences in relation to breaches of expectations and guidelines in the school's Responsible Behaviour Plan. The school may consider the willingness of the responsible student (and/or their parents) to repair or replace the damaged item when making decisions about school consequences. The parents/guardians of students whose device has been damaged may also choose to report this damage to police or take legal action to recover costs to repair or replace the damaged device.

- The school will educate students on cyber bullying, safe internet and email practices and health and safety regarding the physical use of electronic devices. Students have a responsibility to incorporate these safe practices in their daily behaviour at school.

The school's BYOD program supports personally-owned mobile devices in terms of access to:

- printing
- internet
- file access and storage
- support to connect devices to the school network.

However, the school's BYOD program does not support personally-owned mobile devices in regard to:

- technical support
- charging of devices at school
- security, integrity, insurance and maintenance
- private network account

# LAIDLEY SHS Digital Futures

## Responsible Use Agreement 2022

**The following is to be read and completed by both the STUDENT and PARENT/CAREGIVER:**

- I have read and understood the Laidley State High School Digital Futures Guidebook and the school Responsible Behaviour Plan.
- I agree to abide by the guidelines outlined by both documents.
- I am aware that non-compliance or irresponsible behavior, as per the intent of the Digital Futures Guidebook and the Responsible Behaviour Plan, will result in consequences relative to the behaviour.

*In signing below, I acknowledge that I,*

☐ Want my child to participate in the **BYOD PROGRAM**. I understand that there is no charge for my child to access this component of the Digital Futures program.

**OR**

☐ Want my child to participate in the **LAIDLEY SHS LAPTOP HIRE PROGRAM** and agree to pay **$300** for my child to access this component of the Digital Futures program.

**OR**

☐ Am **APPLYING** for my child to participate in the **LAIDLEY SHS EQUITY PROGRAM** and agree to contribute (if accepted) **$100** for my child to access this component of the Digital Futures program.

- Understand that the Laidley SHS Hire Program and EQUITY Program are paid on a pro-rata basis from the date of joining the program
- Accept that students will be invoiced the associated program cost upon commencement in program
- Accept all policies and guidelines as per the Responsible Behaviour Plan for Students and The Laidley SHS Digital Futures Guidebook
- Understand and agree to my responsibilities regarding the use of the device and the internet
- Understand and agree with all of the conditions detailed in the Digital Futures Guidebook
- Understand that failure to comply with the Responsible Use Agreement could result in loss of access to the school's ICT network
- Agree to pay for the cost of repairs to Laidley SHS Hire and EQUITY Hire devices unless deemed to be due to manufacturing fault *(please see over for more details*)

| Care Class | Student's name | Signature of student | Date |
|---|---|---|---|
| | Parent / caregiver's name | Signature of parent / caregiver | Date |
| | Designated school representative's name | Signature of school representative | Date |

***Office Use only***

Date of device / program set up: _____

Date Invoiced processed: _____

**Changes to program**

***Old Program***

☐ BYOD ☐ Hire program ☐ EQUITY

***New Program***

☐ BYOD ☐ Hire program ☐ EQUITY

## Laidley SHS Laptop Hire and EQUITY Repairs

As part of these programs students will have access to a Laidley State High School owned device that is connected to the school's network for internet access (with content filtering), network storage and printing services. While at home the device is able to be connected to the home network where it can access personal networks, internet and printing devices.

While the device is hired to a student it is important to understand that it is the responsibility of the student and family, and as such, **any damages incurred will result in the student being invoiced for the cost of repairs**.

As these devices are under warranty they cannot be repaired by an outside agency and must be returned to the school in order for a job to be logged with the manufacturer.

All devices owned by Laidley SHS will incur the following charges when being repaired. If the repair is deemed to be due to manufacturing fault there will be no charge. If a damage is substantial and considered "not economical to repair", the student/family will be required to pay half of the replacement cost of the unit, typically around ~$350

| Item to be replaced | Cost |
|---|---|
| Hard Drive | $200 |
| LCD screen | $100 |
| Keyboard | $50 - 150 |
| Battery (AC adaptor) | $50 |
| AC Port Damage | $70 |

### Process for having a Laidley SHS Hire or EQUITY laptop repaired

1. Complete a Laidley SHS IT Device Incident Report (available from the school library or the school website – www.laidleyshs.eq.edu.au)
2. Take the completed form and device to the Laidley SHS IT staff (in the school library)
3. The device will be assessed by the IT staff and if required logged for repair by the manufacturer
4. The device will be repaired and returned to the student
5. Once the invoice is generated by the manufacturer this will be added to the students account and a letter sent home to parents/guardians

# Laidley SHS Digital Futures

# Device Incident Report

This form should be completed when reporting an incident relating to a school owned device.

**Student Name:** _____

**Nature of Incident:**

☐ **Malfunction** ☐ **Damage**

**Date of Incident:** / / **Time:** :

**Location:** _____

**Description of Incident:**

Include details of where the device was at the time and full of what occurred.

- If the device is not working, describe what the problem is and if you know what may have caused the problem.
- If accidental damage, describe the incident and the damage.

_____

_____

_____

_____

_____

**Have you backed up your hard drive data?** ☐ Yes ☐ No

*This is in case your device needs to be reimaged or replaced and data will be removed.*

| | | |
|---|---|---|
| | | |
| **Student's name** | **Signature of student** | **Date** |
| | | |
| **Parent / caregiver's name** | **Signature of parent / caregiver** | **Date** |