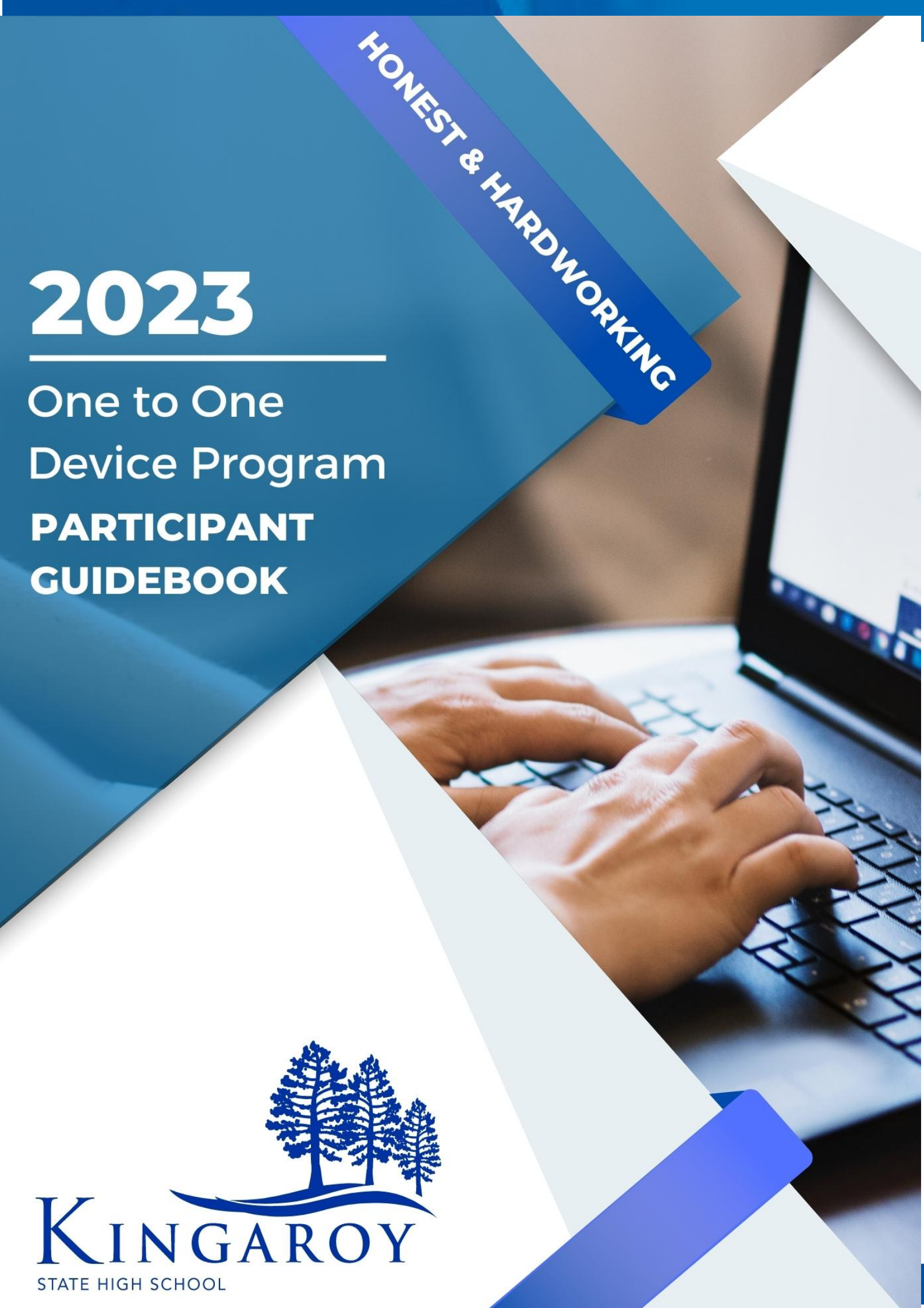
HONEST & HARDWORKING

2023

One to One Device Program

PARTICIPANT GUIDEBOOK



KINGAROY
STATE HIGH SCHOOL

Contents

Kingaroy SHS - One to one device program

Overview

Information and communication technologies (ICT) are an important part of contemporary schooling. The Australian Curriculum includes ICTs as a general capability across all learning areas, as well as Digital Technologies as a specific learning area. A one to one device program ensures that all students have access to a device at any time.

The wind down and removal of government support for computers in schools has brought about many challenges. We have continued to work through these challenges to offer the best possible value and learning experience for our parents and students.

To address the shortage, Kingaroy SHS has chosen to implement a one to one device program, to ensure students have access to a dedicated electronic device to enhance their learning experiences both at home and at school.

Our aim is to ensure that all students starting at Year 7 have a device, that will last for three years before being replaced in grade 10 for the final three years of high school. Students at our school will continue to have the option of participating in the BYOD program.

Our student resource hire fee is structured to provide quality service and products whilst maintaining value for money for families of Kingaroy SHS. The One to one device program fee for 2023 will be $300 per year (payment plans available) and our aim is that this will stay the same for all grades.

Device for hire

Each laptop will be:

- commercial grade
- protected by Education Queensland anti-virus tools and automated updates
- covered by warranty including the battery
- able to be connected to the Education Queensland Network and have filtered internet and email
- able to be used at home and at school for student learning
- installed with central data storage, common file access, backup and network software resources
- repaired through the school, where possible, including software and hardware repairs
- exchanged for a temporary laptop during any repair and maintenance (unless unavailable)

One Education Infinity Device.

The perfect Windows 10 classic laptop for education with its combination of ruggedness and long battery life it's ideal for modern classrooms.

- ultra-low voltage processor
- Intel processor
- 8 GB memory
- 11.6 screen
- 256 GB SSD Storage
- Integrated webcam
- 6-hour battery+
- 3-year warranty
- Accidental damage protection
- Crush-proof protective case

BYOD Specification Requirements

When a device is used here at school we need to ensure that the specifications are suitable to run the programs and software efficiently.

Outlined below is the minimum standard specifications however the device needed for your child may require higher specifications as selected subjects (Digital Solutions, Visual Art, Film Television and new Media, etc.) use software that is more demanding on the system.

It may be necessary to look into a device that has a faster processing speed and memory capabilities.

Minimum specifications for a device to be used at our school are:

- 5GHZ Wireless
- Modern Mobile CPU (Core i3 or similar)
- 8GB or more of RAM
- 8hrs or more Battery Life
- Accidental Damage Protection
- Protective Case
- Windows 10 only – No Chrome OS, iPad, Android or Win10 S

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 of a device at home, in transit or at school belongs to the student (parent) and will incur a replacement fee. Accidental damage protection insurance is provided however there is an excess fee of $50 per claim.

General care 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 included 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 the 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 in a way that could press against the screen or put pressure on the screen. ie the power charger
- 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 regularly and securely. Otherwise, should a hardware or software fault occur, assignments and the products of other class activities may be lost.

Students should always have all documents in a minimum of two locations. These are the location available to our students.

1. On the device, on the hard drive (documents, videos, pictures, etc)
    a. Accessible anytime you have that device, no backup

2. OneDrive cloud storage via student Office365 EQ account
    a. Accessible anytime, anywhere, on any device and automatically backed up
3. Saved into the students Home Drive (H Drive) on our school server
    a. Accessible only at school but automatically backed up
4. A copy on a USB or external hard drive
    a. Accessible anytime, anywhere, on any device, no backup

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

Students should also be aware that, in the event that any repairs need to be carried out the school technician 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 device use

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

This policy also forms part of this One to one device program. 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 school's Student Code of Conduct available on the school website.

While using the school device at school or home, 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 each term, 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. Passwords are required to be at least eight characters long with a combination of lower- and upper-case letters, numbers and symbols.

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 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. 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 'Cybersafety Help button' 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 schools the Student Code of Conduct. 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.

When connected to home networks, mobile hot spots or other internet sources, devices do not have the web filtering applied. Parents/caregivers are responsible for appropriate internet use by students outside the school. Parents, caregivers and students are also encouraged to visit the website of the Australian eSafety Commissioner 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

The device will be preloaded with required software for Kingaroy SHS. Parents/caregivers may be required to install and support the appropriate use of the software in accordance with guidelines provided by the school. Students will be able to visit tech services in The Resource Centre at any break time or before school for help around software for classes.

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.

For more information about the One to one program, please email:

byod@kingaroyshs.eq.edu.au