



Student BYOD Charter

Contents

BYOD Program at Holland Park State High School.....	3
Device selection	4
Responsible use of BYOD.....	6
Acceptable personal mobile device use.....	7
Passwords.....	8
Digital citizenship.....	8
Cybersafety	9
Web filtering.....	9
Privacy and confidentiality	10
Intellectual property and copyright.....	11
Software	11
Monitoring and reporting.....	11
Misuse and breaches of acceptable usage.....	11
Device care	14
Data security and back-ups	14
Support at HPSHS.....	15
Agreement re Short Term Loan (Emergency) & Responsible use agreement.....	16

BYOD Program at Holland Park SHS

The BYOD program is offered to all students in years 7-12 and allows students to bring a privately-owned laptop to school every day for use in class.

Our BYOD program assists students to improve their learning outcomes in a contemporary educational setting and recognizes the demand for seamless movement between school and home. By supporting students to become responsible digital citizens, student outcomes are enhanced as well as the skills and experiences that will prepare them for their future studies and careers.

Microsoft Intune

Access to school's network is managed through Microsoft Intune - a DETE approved BYOD on-boarding system. Enrolling your child's device via Intune involves installing an authentication certificate that grants secure connection to the school BYOD network. Once onboarded the student will have access to filtered internet, network storage/sharing and printing facilities.

Intune does NOT allow staff to

- see personal information,
- monitor what happens on the device,
- track or locate the device,
- see information on installed non-school applications
- uninstall applications, including personal ones.

Steps to joining the BYOD Program

1. Read and understand this BYOD Student Charter and the School's Student Code of Conduct.
2. Return the signed Short Term Loan and Responsible Use Agreements (you may have already submitted a copy of the BYOD Agreement as part of the enrolment pack) to Admin or the I.T. Support desk (located in the Library).
3. Purchase a suitable device as per BYOD device selection below
4. Setup and onboard the laptop as per information on [BYOD webpage](#) or with I.T. support assistance.

Device selection

Laptops are the chosen device for teaching and learning at our school.

These specifications below relate to the suitability of the laptop to enabling class activities, meeting student needs and promoting safe and secure access to the department's network.

Minimum Laptop Specifications

- Screen: 12-inch (measured diagonally)
- Operating System: Windows 10 / Mac OS 11.0 (Big Sur)
- CPU (Processor): Intel Core i3 or AMD Ryzen 3
- Memory (RAM): 4GB
- Storage: 128GB Solid State Drive (SSD)
- Network: Dual Band Wireless [802.11ac (2.4/5.0GHz)]
- Battery: Minimum 6hr run time on balanced power setting
- Hard Case Carry Bag

Higher End Laptops

Students studying Art, Graphics and Music should consider a device for higher level computing (see specs below). HPSHS will utilise applicable software in these classes. This software will be supplied and installed by the school and may incur extra charges under subject levies.

Recommended Specifications

- CPU: Intel Core i5 or AMD Ryzen 5 or Higher
- Memory: 16GB or higher
- Storage: 256GB Solid State Drive (SSD) or higher

If you wish to discuss specifications or seek further clarification please contact
HPSHS I.T. Support (3347 0111) or email
StudentITSupport@hollandparkshs.eq.edu.au

Device selection cont..

Not Supported

The following devices are NOT supported at HPSHS.

- **Chromebooks** - These devices are not compatible with BYOD solution.
- **Tablets, iPads or Smart Phones** - These devices are not suitable for learning at HPSHS.
- **Any devices running the following Operating Systems** -
Windows 10 or 11 in S mode (switching out of S mode is free – students can see I.T. staff for assistance if needed), Windows RT, Linux, Unix or any OS not mentioned in the minimum specs above.

Software

- BYOX Connect allows students to access school network drives and printing services. This is supplied and supported by the school.
- Anti-virus software is mandatory on all laptops utilising the BYOD system. The inbuilt security software for Windows and Mac laptops will suffice. However, you may prefer to purchase your own Anti-virus program.
- Microsoft Edge for Windows, Safari for Mac, Mozilla Firefox and Google Chrome are all supported web browsers for use with the BYOD system.
- The Microsoft Office suite is available free for students.
[How to download and install Microsoft Office to a Windows computer \(PDF, 1MB\)](#)
[How to download and install Microsoft Office to a Mac computer \(PDF, 1.3MB\)](#)
- Subject specific software will be supplied and installed by the school.
Note: Some software may incur extra charges under subject levies.

Other Considerations

- Length of warranty
- Accidental damage protection
- How and where repairs are carried out
- Excess for repairs

Responsible use of BYOD at Holland Park SHS

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 BYOD 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 responsibilities table)
- short term Hot Swap device loan facility
- printing facilities.

Student

- participation in BYOD program induction
- 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 [eSafety](#))
- 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)
- accessing technical support (please consult Technical support responsibilities table)
- maintaining a current back-up of data
- charging of device
- 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
- understanding and signing the BYOD Charter Agreement.

Parents and caregivers

- acknowledgment 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 [eSafety](#))
- accessing technical support (please consult Technical support responsibilities table)
- required software, including sufficient anti-virus software
- protective backpack or case for the device
- adequate warranty and insurance of the device
- understanding and signing the BYOD Charter Agreement.

Acceptable use of the Department's Information, Communication and Technology (ICT) Network and Systems

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'

Communication through Internet and online communication services must also comply with the department's [Student Code of Conduct](#).

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 unauthorized 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 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 Student Code of Conduct 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 [eSafety website for kids](#) 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 [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 [Student Code of Conduct](#) 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 Australian Govt. [eSafety Commissioner](#) 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 fulfill 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

Teachers may recommend 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 laptops 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 laptops may result in disciplinary action which includes, but is not limited to, the withdrawal of access to school supplied services.

It is appropriate for students at Holland Park State High School to:

- use devices such as laptops for
 - assigned class work and assignments set by teachers
 - developing appropriate literacy, communication and information skills
 - authoring text, artwork, audio and visual material for publication on the intranet or internet for educational purposes as supervised and approved by the school
 - conducting general research for school activities and projects
 - communicating or collaborating with other students, teachers, parents or experts in relation to schoolwork
 - accessing online references such as dictionaries, encyclopedias, etc.
 - researching and learning through the department's eLearning environment
- be courteous, considerate and respectful of others when using a mobile device
- switch off and place the mobile device out of sight during classes unless the device is being used in a teacher directed activity to enhance learning
- seek school approval where they wish to use a mobile device under special circumstances such as for monitoring a medical condition.

It is unacceptable for students at Holland Park State High School to:

- use a mobile phone or other devices in an unlawful manner
- use any mobile device for any purpose in class without teacher consent
- use a mobile phone in technology-free designated spaces eg. toilets, or times
- download, distribute or publish offensive messages or pictures
- use obscene, inflammatory, racist, discriminatory or derogatory language
- use language and/or threats of violence that may amount to bullying and/or harassment, or even stalking
- insult, harass or attack others or use obscene or abusive language
- deliberately waste printing and Internet resources
- damage computers, printers or network equipment
- commit plagiarism or violate copyright laws
- ignore teacher directions for the use of online email and online collaboration eg. Blackboard
- send chain letters or spam email (junk mail)
- knowingly download viruses or any other programs capable of breaching the department's network security
- use in-phone cameras anywhere a normal camera would be considered inappropriate, such as in change rooms or toilets
- invade 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
- use a mobile phone (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.
- 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.

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 Student Code of Conduct.
- 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.

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 regarding inclusion in home and contents insurance policy.

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

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 may be able to save data to the school's network, 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.

Support at Holland Park SHS

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

- printing
- internet
- file access and storage
- support to connect devices to the school network
- general technical advice and troubleshooting
- Short term loan hot swap laptop

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

- technical support (other than trouble-shooting and advice)
- charging of devices at school
- security, integrity, insurance, repairs and maintenance
- private network accounts.

Repairs:

Warranty and accidental damage repairs on individually owned laptops are the responsibility of parents/caregivers and students.

Repairs on devices purchased from vendors using the school portal must be logged with the vendor by the parent/caregiver or student. Repairs may then be scheduled to be done at school by the authorized vendor technician.

Technical support responsibilities:

	Connection:	Hardware:	Software:
Parents / Caregivers Students	✓ home-provided Internet connection	✓	✓
School	✓ school provided Internet connection	✓ limited to trouble-shooting and advice	✓ some school-based software arrangements
Device vendor		✓ see specifics of warranty on purchase	