Bentley Park College

ASPIRE - LEARN - ACHIEVE

Bring Your Own Device and TechExpress Charter

Queensland Government

CONTENTS

Bring Your Own Device and TechExpress

Bring Your Own Device (BYOD) is a term used to describe a digital device ownership model where students or staff use their personally-owned devices to access the Department of Education and Training's (DET) information and communication technology (ICT) network.

The Bentley Park College BYOD program for Secondary, and TechExpress program for Years 3-6, were developed in response to the significant role technology plays in education. They enable students to bring a personally-owned device to school as a learning tool and provides seamless movement between school and home.

Students wishing to access the program and their parents/carers must have read the Acceptable Use of Information Technology and Virtual Reality Equipment and Systems Policy, and completed an Acceptable Use of Information Technology and Virtual Reality Equipment and Systems Agreement (available on our website).

Secondary
The College strongly recommends all Secondary students have access to their own personal device, with the Secondary Student BYOD Program aiming to encourage a sense of ownership, responsibility and independence as well as improving students' technology skills.

Primary
We also encourage Primary students to have access to their own device and students in Years 3 to 6 can apply for our TechExpress Program. For younger Primary students the P-2 iPad Program is being implemented, with Prep and Year 1 students having iPads in 2022. These programs each have their own charter and agreement where you can find more information.

Why your child needs their own device:

- Enhanced learning and engagement in the classroom.
- Independent learning at home.
- Seamless access to the curriculum, being able to use your own device both at school and at home.
- Increased student participation, opportunities for collaboration and positive engagement during class time.
- Learning becomes student driven.
- Flexible learning options between home and school using a wide range of online learning programs and tools.
- Encourages and supports versatile learning styles and abilities.
- Increases opportunities and access to higher and extended learning.
- Improved Technology skills.
- Includes Microsoft Office at no cost and Adobe Creative Cloud software suite at minimal cost.
- Access to school Outlook email.
- Access to school calendar and information on events.
- Access to ClickView, The Learning Place, OneNote Classrooms and Microsoft Teams.
- Access to Smart Online Learning Suite.
- Access to e-textbooks.
- For Primary: access to Mathletics, Reading Eggs, Scratch.
- For Secondary: access to Mathspace and Mathletics

Access to the ICT network is provided only if the device meets DET's security requirements which, at a minimum, requires that anti-virus software has been installed, is running and is kept updated on the device.

To ensure students have the best possible learning experience, please ensure their device meets the minimum specifications outlined. These are recommendations, with affordability and functionality, accidental protection insurance, and extended warranty, also being critical issues when deciding on a device. The College's BYOD/TechExpress program may support printing, filtered internet access and file access and storage through DET's network while at school. However, the College's BYOD/TechExpress program **does not** include charging of devices at school.

Please note: Smartphones, Android devices, Google Chromebooks, Surface RT and other devices that run Linux are unsuitable for the College environment as they require a connection to Google Drive which is blocked by the Queensland Department of Education.

BYOD/TechExpress Program Device Specifications		
Specifications	**Minimum**	**Recommended**
Physical dimensions	11"	14"
Operating system	Windows 10 or Mac OSx 10.12.x (or newer)	Windows 10
Hard drive/storage	128GB HDD or SSD	256GB SSD (or larger)
Memory	4GB RAM	8GB RAM
Wireless capability	WiFi 802.11n/ac (5Ghz)	
Warranty		3+ years warranty 3+ years accidental damage protection
Battery life	Advertised battery life of at least six hours	
Software	Microsoft Office (available at no cost for students) **Anti-virus** - Windows Security (up to date) is available as part of Windows and has proven to be suitable and is free. You may want to purchase extra cover.	
Software (optional)	Adobe Creative Cloud – available to all students at a price of $10 per year	
Other	Extra chargers Bag Mouse	

Software

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

Some software the College has purchased is allowed to be installed onto students take home devices under special vendor agreements. All applications and shortcuts provided by the College are for educational purposes only. The following is a list of applications and their purpose:

- **BYOD/TechExpress Portal** – this application allows the device to connect to the school's printers and network drives
- **Microsoft Office:** Under Education Queensland's agreement with Microsoft, students can now freely access Microsoft Office 365 for Mac, Windows and iOS. Go to the website http://login.microsoftonline.com login with the student email address and download the software

Any privately-owned software installed on the device must be age appropriate, follow copyright legislation and not cause offence.

Note on Windows 10 in s-mode

Windows 10 S-Mode is a version of Windows 10 designed for security and performance, exclusively running apps from the Microsoft Store. In order for the device to connect to the BYO Network, the device will need to be switched out of S-Mode. Instructions are available on the Microsoft support website at https://support.microsoft.com/enus/help/4456067/windows-10-switch-out-of-s-mode.

Possible Device Provider Options	
Acer https://byod.acer.com.au/school/qld/byod-store/notebooks	Three-year on-site warranty (repairs are done at school)
Brilliant Computers Phone: (07) 4052 5933 | 147-151 Mulgrave Road, Cairns, 4870	Bundles are available with three-year on-site warranty and accidental damage protection (repairs at school or at their workshop), and protective carry bag.
JB Hi-Fi https://www.jbeducation.com.au/byod/	School code: **bentleypark2021**
Harvey Norman https://www.harveynorman.com.au/studentdevices	Product Care Replacement Plans are available

Student Laptop Hire Program

A limited number of devices are available for students to hire. To apply to participate in the Student Laptop Hire Program, students and their parent/carer must read and understand the required documentation, including the Primary and Secondary Student Laptop Hire Program Charter, and complete either the Primary or Secondary Student Laptop Hire Program Charter Agreement. Fees apply.

Device Care and Usage Guidelines

Students are responsible for taking care of and securing their device and accessories in accordance with College 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.

- Consider engraving the device – engraving the bottom of the laptop with the student's name will help school staff to locate lost laptops and return them to their owners.
- Don't have food or drink near the laptop.
- Ensure your laptop is fully charged each day.
- Gently place the laptop on a stable surface before switching on.
- Take care when using the laptop. Avoid dropping or bumping the machine. Only connect the adapter supplied to your machine. Never use an adapter belonging to another machine.
- Do not wrap the cord tightly around the adapter box and when unplugging the power cord, pull on the plug itself, not the cord. All plugs, cords and cables should be inserted and removed carefully.
- Computer batteries can become hot during use. Do not use the computer on your lap.
- Avoid moving your laptop around when it is turned on and always package, carry and store the laptop in its carry case for transportation. Turn the device off first.
- Keep the laptop with you at all times. Should students need to leave the laptop unattended it needs to be stored in a secure location.
- Screen protection: don't poke, prod, push or slam the LCD screen and never pick up the laptop by its screen. Don't place pressure on the lid of the device when it's closed, avoid placing anything on the keyboard before closing the lid and avoid placing anything in the

carry case that could press against the cover. Only clean the screen with a clean, soft, dry cloth or anti-static cloth (not with household cleaning products).

Hire Laptops Only

- If a hire laptop is accidentally damaged students must report the damage immediately to administration personnel. If damage occurs to the laptop the school will determine when and/or if a replacement machine is made available to the student.

Data security and back-ups

Students are responsible for the backup of all data and 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.

While at school, students may be able to save data to the school's network, which is safeguarded by a scheduled backup solution. Students are also able to save data locally to their device for use away from the school network.

Information should also be backed-up to an external device such as an external hard drive or USB drive, or backed up to a cloud location such as Microsoft OneDrive. 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.

Acceptable Computer and Internet Use

Communication through internet and online communication services must comply with the Acceptable Use of Information Technology and Virtual Reality Equipment and Systems Policy, and the Bentley Park College Student Code of Conduct, both available on our website.

Students should be aware they are held responsible for their actions while using the internet and online communication services and for any breaches caused by other people knowingly using their account. Misuse may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

Note: use of internet and online communication services can be audited and traced to the account of the user.

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.

Passwords

Use of the school's ICT network is secured with a username and password. The password must be difficult enough so as not to be guessed by 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 or staff).

- 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 set a password for access to their BYOD and keep it private.
- Students should log off at the end of each session to ensure no one else can use their account or device.

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 today 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/carers are requested to ensure that their child understands this responsibility and expectation.

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 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 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/carers and students are encouraged to read DET's Online Safety in Queensland State Schools.

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. The DET operates a web filtering system to protect students and restrict access from malicious web activity and inappropriate websites.

When students are connected through DET managed networks (including the BYOD network) they will have a high level of filtering applied. This level restricts them from websites such as:

- social networking sites e.g. Facebook, Instagram, Twitter etc.
- open/mixed content sites e.g. YouTube
- translation sites e.g. Google translate
- chat sites
- internet telephony and video conferencing sites e.g. Skype, Zoom etc.
- document sharing and cloud storage e.g. Prezi, iCloud, Google Drive
- peer to peer sites and downloading services e.g. Bit Torrent, uTorrent, Pirate Bay, Kazzaa etc.

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 College'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.

WARNING: Outside of the DOE network, i.e. home or 3G/4G tethering to a mobile phone; is not filtered. Parent/Carer vigilance is a must when students are browsing the internet away from school to ensure students are not looking at inappropriate websites. Under the Bentley Park College BYOD program, tethering of a personal device or connecting to an unfiltered 3G or 4G connection during school times is strictly prohibited.

Students' Reporting Requirements

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 DET network must also be reported to the College.

Privacy and confidentiality

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. The student should not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. It should also be ensured 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.

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 College staff. If at any stage there is a police request, the College 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 people knowingly using their account to access internet and online communication services.

The misuse of internet and online communication services, including accessing inappropriate sites as deemed so by the College, may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services, school disciplinary absences or involvement of the Queensland Police Service.

The College 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 Responsible use of BYOD/TechExpress at Bentley Park College

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/TechExpress program:

College

- BYOD/TechExpress program induction – including information on connection, care of device at school, workplace health and safety, appropriate digital citizenship and cybersafety.
- Wireless connectivity to the school's network via a security certificate and network password.
- Internet connection and Internet filtering (when connected to the school's computer network)
- Some technical support.
- Printing facilities.
- Access to network drives.

Student

- Participation in BYOD/TechExpress program induction.
- Understanding and signing the BYOD/TechExpress Charter Agreement.
- Acknowledgement that the core purpose of the device at school is for educational purposes.
- Internet filtering (when not connected to the school's network).
- Care of the device.
- Ensuring device is fully charged before attending school.
- Security and password protection.
- Maintaining a current back-up of data.
- Appropriate digital citizenship and online safety (for more details, see ACMA CyberSmart website).
- Abiding by intellectual property and copyright laws (including software/media piracy).

Parents and carers

- Understanding and signing the Acceptable Use of IT and VR Agreement.
- Acknowledgement that the core purpose of the 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 ACMA CyberSmart website).
- Some technical support e.g. home internet connection.
- Any repairs required.
- Required software, including sufficient anti-virus software.
- Protective backpack or case for the device.
- Adequate warranty and insurance of the device.

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

- Using devices for:
    - engagement in class work and assignments set by teachers
    - developing appropriate 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 and collaborating with other students, teachers, parents, carers or experts as part of assigned school work
    - accessing online references such as dictionaries, encyclopaedias etc.
    - researching and learning through the College's eLearning environment
- Being courteous, considerate and respectful of others when using a mobile device.
- Ensuring the device is fully charged before bringing it to school to enable continuity of learning.
- Switching off and placing out of sight the device during classes, where these devices are not being used in a teacher directed activity to enhance learning.
- Using the personal device for private use before or after school, or during recess and lunch breaks.
- Seeking teacher approval where they wish to use a 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 bulling 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 school 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 sharing etc.) of such material.
- Using the device (including those with Bluetooth functionality) to cheat during exams or assessments.
- Take into or use devices at exams or during class assessment unless expressly permitted by school staff.

School contacts

If you have any questions or require any further information regarding the Secondary Student BYOD Program, please do not hesitate to contact the College. The IT Support Room is open for students during school hours if they require assistance.