BYOx – Everything parents need to know

2022

Western Cape College

Email: admin@westerncapecollege.eq.edu.au
Website: https://westerncapecollege.eq.edu.au

Tel: (07) 4090 6444
Central Avenue, Weipa Qld 4874

Table of Contents

WESTERN CAPE COLLEGE – "E-LEARNING PROGRAM" 2
BYOX PROGRAM 2
OTHER FACTORS INVOLVED WITH BYOX 2
WHEN TO PURCHASE? 2
BYOX DEVICE SELECTION 2
MINIMUM HARDWARE REQUIREMENTS FOR DEVICE SELECTION 3
BYOX VENDOR PORTAL 3
WCC EQUITY PROGRAM 4
SETTING UP YOUR DEVICE FOR BYOX 4
ENSURE THE ACCOUNT TYPE IS AN ADMINISTRATOR ON WINDOWS 10: 4
ENSURE THE ACCOUNT IS PASSWORD PROTECTED 4
ENSURE THE TIME ZONE IS CORRECT 4
ENSURE VIRUS PROTECTION IS ENABLED 4
DOWNLOAD OFFICE 365 5
DEVICE CARE AND MAINTENANCE 5
DATA RESPONSIBILITIES 5
ACCEPTABLE PERSONAL MOBILE DEVICE USE 5
PASSWORDS 6
DIGITAL CITIZENSHIP 6
CYBERSAFETY 6
WEB FILTERING 7
PRIVACY AND CONFIDENTIALITY 8
INTELLECTUAL PROPERTY AND COPYRIGHT 8
SOFTWARE 8
MONITORING AND REPORTING 8
MISUSE AND BREACHES OF ACCEPTABLE USAGE 8
RESPONSIBLE USE OF BYOX 9
CASE / CARRY BAG 11
LOCKER HIRE 11
FEE PROVISION OF BYOX PROGRAM 11
SCHOOL SUPPORT 12
CHECK LIST 12
BYOX USER AGREEMENT 13

WESTERN CAPE COLLEGE – "E-LEARNING PROGRAM"

The demands of 21st century teaching and learning are increasing the usage of technology in class to the point where it is realistic to expect that a student should have access to a device at all times. This necessitates a 1-1 student – device ratio.

Western Cape College (WCC) believes that it is important to learn valuable knowledge and also the skills to help students succeed in the future. In order for this to occur effectively and equitably, WCC has proposed three possible options to enable students to be part of the E-learning vision.

1) Bring Your Own existing device
2) Buying a new device
3) WCC Equity Scheme

BYOX PROGRAM

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

Other factors involved with BYOx

The school's BYOx program does not include charging of devices at school. It will be expected of students to ensure their **device is fully charged** for the start each school day.

Apple OS laptops can be brought to school but minimum support will be provided for them as Western Cape College is a Microsoft Windows supported school.

WHEN TO PURCHASE?

WCC expects all students to have an IT device ready for the first day of school – 24 January 2022. It is recommended that you purchase a device by the end of the year. This way students can become familiar with the device and be ready to learn on it when school resumes next year.

BYOX DEVICE SELECTION

Before purchasing 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 enable class activities, meet student needs and promote safe and secure access to the department's network.

NB: If you already own a functioning laptop, it can be brought to school as a learning device. Please make sure it meets the minimum requirements, or contact our IT team to analyse your device.

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 -

Device Specification	Minimum Specification
Platform	Microsoft Windows
Processor	Intel i3 or higher
Storage	Internal Hard Drive, or Solid State Drive. 128Gb or greater
Operating System	Windows 10
RAM	4GB or higher
Wireless	5GHz Wi-Fi 802.11n – minimum 802.11ac – recommended
Battery	6 hours working life
Ports	USB, audio in/out, in-built microphone, VGA or HDMI, camera, SD card
Warranty	3 years
Accidental Damage Protection	Highly Recommended
Anti-Virus	Minimum: Windows Defender **Recommended**: students are eligible for a discounted Norton Security Deluxe at https://detstudent.onthehub.com Students sign on with their EQ login details.

BYOX VENDOR PORTAL

WCC are teaming up with Dell to assist parents/caregivers to purchase a suitable new device for the BYOx program. Choosing a device that is the right fit can be a tedious task, this is why we have set up a portal to assist you through the selection process. Purchasing a device through the Dell Vendor portal guarantees:

- Your laptop will be supported at WCC
- Comes with a 3 year on-site warranty with ADP
- Free Shipping
- Students have full ownership of their device
- Ongoing support from Dell

Additional options through the Dell portal include:

- Flexi payment options available, eg GEM
- Accessories (bags and cases) – highly recommended

If you choose to opt in through the BYOx vendor selection, the WCC technical support team can:

- Provide a laptop skin selection for unique customisation.
- Provide diagnostic advice that may be reported back to the vendor.

The vendor allows the IT team at WCC to support warranty jobs, but they will not alter the device unless parents give permission to do so. If you are interested in purchasing a device through the portal, click on the link below and use the logon details:

- https://datashop-qld.datacom.com.au/wcc
  - Username: wcc
  - Password: parent

WCC EQUITY PROGRAM

The WCC Equity Program allows families who may be experiencing financial difficulties the ability to work with the school to provide devices for their student/s. To see if you are eligible for an equity device, it is recommended that you book an appointment with Mr Dan Tonon, Associate Principal - Secondary or Mr Craig Law, Associate Principal - Primary to discuss this option further.

SETTING UP YOUR DEVICE FOR BYOX

Once you have your device there are a few steps to ensure it is ready for BYOx. Please follow these steps below:

Ensure the account type is an Administrator on Windows 10:

a) Click on Windows and open Settings
b) Click on "Accounts"
c) A page will open with your user information. Under the account name it will display "Administrator" if you are one. If it doesn't say you are an administrator, continue with the steps below:
d) Click on "Family & other people"
e) Select the desired user account
f) Click the change account type button
g) Select the Administrator or Standard User account type depending on your requirements.
h) Click the OK button.

Ensure the account is password protected

a) Usually the password is set up when you initially set up your computer. However if you need to change or add a password.
b) Click on Windows and open Settings
c) Click on "Accounts"
d) Click on "Sign-in options"
e) Under the Password header, you can add or change your current password.

Ensure the time zone is correct

a) Click on Windows and open Settings
b) Click on "Time & Language"
c) Ensure the right time zone is selected "(UTC + 10:00) Brisbane"

Ensure Virus Protection is enabled

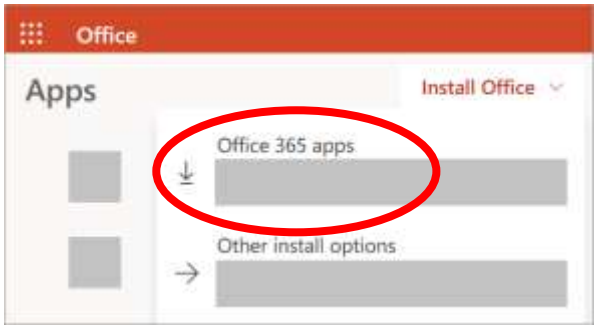
a) Click on Windows and type "Windows Defender Security Centre"
b) Open Windows Defender Security Centre
c) When the new window opens, along the left panel, click on the shield icon
d) This will show you what current virus protection your machine is using
e) Please enable Windows Defender if you do not have a different virus protection installed.

Download Office 365

WCC advises parents to ensure their laptops are equipped with the right programs for BYOx. An essential program required is Office 365. Students are entitled to download their free copy of Office 365 using their Education Queensland login credentials. To sign in and download Office:

1. Go to www.office.com and if you're not already signed in, select Sign in.
2. Sign in with your student EQ login account (if you forget what this is, contact the school)
3. After signing in, follow the steps that match the type of account you signed in with.
4. From the Office 365 home page select **Install Office**

5. Select **Office 365 apps** to begin install.
6. For further support click on this link and follow the instructions.
    a. https://support.office.com/en-us/article/download-and-install-or-reinstall-office-365-or-office-2019-on-a-pc-or-mac-4414eaaf-0478-48be-9c42-23adc4716658



DEVICE CARE AND MAINTENANCE

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 on your 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.

All maintenance for the IT device, operating system, software and/or apps purchased by the family are the responsibility of the family. If a student's laptop is in for repair for an extended period of time, the school may have a loan laptop to support the student's ongoing learning.

DATA RESPONSIBILITIES

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.

Education Queensland students are allocated a large storage space on the Microsoft OneDrive. This can be accessed through www.office.com after signing in. Students can store files online and access those files from any device that has access to the internet and the OneDrive app.

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 BYOx 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 Student Code of Conduct 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). Other factors involving password use include:

- 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.
- 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 '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. 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 Communications and Media Authority's CyberSmart website for resources and practical advice to help young people safely enjoy the online world.

N.B. Tethering of a personal device or connecting to an unfiltered 3G/4G connection during school times is strictly prohibited. Behavioural consequences are in place for any student who breaches this policy.

PRIVACY AND CONFIDENTIALITY

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

Schools 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 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 BYOX

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 BYOx Program:

School

- BYOx 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 BYOx Charter Agreement.
- Lockers for device security

Student

- participation in BYOx 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 ACMA CyberSmart)
- 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
- 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 BYOx Charter Agreement.

Parents and caregivers

- participation in BYOx program induction
- 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 ACMA CyberSmart)
- some technical support (please consult Technical support table below)
- 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:

- 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 private use before or after school, or during recess and 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.

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.

CASE / CARRY BAG

A strong carry case is a great way to protect your device from accidental damage like drops. Use a bag or case designed to hold a laptop with adequate padding.

LOCKER HIRE

Lockers will be available for students to place their bags in. This way the school can ensure a level of protection and storage for laptops during lunch times when the laptops won't be in use.

FEE PROVISION OF BYOX PROGRAM

To participate in the BYOx program parents and/or caregivers are required to make a contribution. This helps to offset the costs involved in the setup, support, and software licenses for the device. The items below are included as part the BYOx package:

Item	Annual cost per student
Device setup for connection by IT support staff	Included
Access to filtered Internet connection within the School	Included
Access to the School printing system	Included
Locker use	Included
Unique laptop skin	Included

$50** will be charged per device, annually.

SCHOOL SUPPORT

If you go to the WCC website https://westerncapecollege.eq.edu.au, open 'Subjects and Programs' under the Curriculum tab, you can find further information about BYOx. By clicking on 'BYOx', you will find documents that have been presented at the BYOx parent evenings. If you would like further information, please contact the IT team via email if you have any further questions. They are happy to answer any queries: BYOxInfo@westerncapecollege.eq.edu.au.

CHECK LIST

Use this check list to ensure you have prepared your BYOx device for 2022. Please ensure all boxes are ticked before proceeding to the User Agreement.

- ☐ Obtain a device
- ☐ Ensure it meets the minimum specification requirements
- ☐ Have an account set up with administrator status
- ☐ Have a password set up with the account
- ☐ Ensure the time zone is correct
- ☐ Ensure laptop has virus protection
- ☐ Ensure Office 365 is downloaded on the device
- ☐ Read and sign this charter to return form to IT Staff at WCC

BYOX USER AGREEMENT

This Student BYOx Agreement form must be signed and returned to the school before the device will be authorised and connected to the school network. The student and parent or caregiver must carefully read this charter before signing it. Any questions should be addressed to the school and clarification obtained before the charter is signed. When you have returned the BYOX charter to the school office, you will be issued with an invoice. Once your invoice has been paid your child can bring their laptop to the IT Department for the set up to be completed.

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

- I have read and understood the BYOx Document.
- I agree to abide by the guidelines outlined in the document.
- I am aware that non-compliance or irresponsible behaviour, as per the intent of the BYOx Document, will result in consequences relative to the behaviour.
- Accept responsibly for any loss, theft or damage that may occur to the device within the School and have insured the device.
- Agree to contribute **$50 annually** for my child to access the BYOx Program plus the cost of any optional software and additional printing.
- Hand this charter signed to the WCC IT staff so they can commence on-boarding the device.

Student's name: _____ **Year:** _____ **ID No** _____

Student's Preferred Locker Combination: _____

Student's signature: _____ **Date:** / /

Parent's/caregiver's name: _____

Parent's/caregiver's signature: _____ **Date:** / /

IT Representative name: _____

IT Representative Signature: _____ **Date:** / /