GUIDELINES FOR PROPER CARE OF THE BYOD

SECURITY AND STORAGE

When the BYOD is at the College, students must always know the location of their BYOD and are responsible for ensuring its safe keeping.

BYODs must also be under the student's direct care during recess and lunchtime. When the computer is not required in class, for example during Physical Education, it is to be placed in a teacher designated secure area.

When the BYOD is being used away from the College, students should avoid leaving it unattended or where it is visible to the public (e.g. in a vehicle). In these circumstances, the BYOD can be a target for theft.

TRANSPORT AND HANDLING PROCEDURES

When transporting the BYOD, students are to make sure that it is protected by either a specially designed protective sleeve or a sleeve built into a backpack or bag. Students are encouraged to take responsibility for the safe handling of devices when transporting the device to and from the College.

GENERAL CARE OF THE BYOD

It is the student's responsibility to maintain the BYOD in good condition.

Technical support is not provided or available for devices / hardware or software problems that may occur with devices (it may void any warranties you may have). Limited support is available for software specifically provided by the Department of Education and/or Ballajura Community College.

The College provides FAQ sheets (available via our website) for connection to our network, installation of required software, and suggestions on overcoming common issues.

Students will be assisted with establishing a connection to our network and printing, if required.

REPORT OF LOSS OR DAMAGE

In circumstances where deliberate damage or theft has occurred, it is the student's responsibility to report the incident to the Police.

DATA MANAGEMENT

Saving and backup of data is the student's responsibility. To backup work it is recommended that students use the cloud storage (OneDrive) provided by the College or purchase a USB flash drive or an external hard drive.

Staff will not accept data loss as an excuse for late submission of work.

PRINTING

Wherever possible, we are committed to delivering and receiving electronic forms of class work and assessment. Students must endeavour to produce and submit work and assessments electronically.

Students unable to submit work electronically will be encouraged to print work at home for submission to their teacher. Students should always minimise printing by print-previewing, editing on screen rather than on printouts and spell-checking before printing.

Students will have limited access to network printers. Print credit will be allocated, and each page printed will incur a charge against this. Once used, print credit will need to be topped up by students.

VIRUS PROTECTION

The BYODs should be configured with anti-virus software which regularly and automatically checks for viruses on the device.

ACCESS SECURITY

It is a condition of entry into the student BYOD program that students agree to the monitoring of all activities including their Department of Education email and internet use.

MONITORING, LOGGING AND OPERATIONAL UPDATES

A log of all access to the internet including DoE email will be maintained and may be accessed if required to ensure that undesirable internet sites have not been accessed and that the content of email remains within the guidelines described in this document.

HEALTH AND SAFETY

OCCUPATIONAL HEALTH AND SAFETY GUIDELINES

Basic health and safety guidelines for desktop computers also apply to BYODs use:

- Keep the upper arms relaxed at the side of the body.
- Bend the elbows to around 90 degrees.
- Keep wrists straight.
- Change position every 15-20 minutes and take a complete break to get up and move body every 30-60 minutes.
- Avoid prolonged use of computers/devices/laptops.
- Students with special needs will be catered for according to Department of Education guidelines

CYBER SAFETY

The College maintains safeguards against student access to unsafe and inappropriate websites and can monitor students' activity so long as they are connected to the internet via the College network. Therefore, hot spotting to personal devices is not permitted.

The College cannot monitor communications sent or received through third-party software and applications such as social media. Students and parents must report any negative experiences, including instances of bullying or harassment, to College staff.

Parents will be aware of many incidents reported in the media regarding safety online. Personal information is easily tracked and harvested by those who know how, so it is important to keep as safe as possible while online.

Parents are encouraged to check the following website for further useful information:
www.esafety.gov.au

WHAT DO I NEED TO DO NOW?

- Ensure you have read this document and the ***Ballajura Community College: Acceptable Use of ICT Agreement***.

- Discuss the information, rules, procedures, and responsibilities for appropriate use with your child. It is essential they understand that this privilege is subject to following the rules and procedures as described, both at the college and at home.

- Before purchasing or providing a device, check it has the BYOD MINIMUM SPECIFICATIONS.

- Ensure your child takes the signed ***Ballajura Community College: Acceptable Use of ICT Agreement*** to main administration staff. A BYOD setup document will be made available on the BCC website.

- Keep a copy of this document for your records. An online version is available through the BCC website.

- Check that the device is adequately insured and read the user manuals and information provided by the manufacturer.

- Spend time with your child familiarising yourselves with the operation of the device and establishing appropriate behaviour and expectations at home.

- If you have questions or concerns, please contact the College by emailing ballajura.cc@education.wa.edu.au