



Albany Senior High School

Bring Your Own Device (BYOD)

Usage Policy & Guidelines

Updated September 2019

Table of Contents

1	Introduction	1
2	Description and Purpose of the Project	1
3	Responsibilities	2
	3.1 The Role of Students	2
	3.2 The Role of Parents or Guardians	2
	3.3 The Role of Teaching Staff	2
	3.4 The Role of the school	2
4	Authorisation and Rules for Home Use	3
	4.1 Security, Transport and Storage	3
	4.2 Occupational Health and Safety Guidelines	3
	4.3 Loss or Damage	3
5	Data Management	3
6	Printing	3
7	Virus Protection	3
8	Acceptable Use Policies	4
	8.1 Access Security	4
	8.2 Monitoring and Logging	4
	8.3 Internet Usage	4
	8.3.1 Chat lines (IRC, MIRC, ICQ etc)	5
	8.3.2 Cyber safety	5
	BYOD Specification (Appendix A)	6
	BYOD Usage Policy Agreement (Appendix B)	7

1 INTRODUCTION

The integration of notebook computers and supporting information technology equipment into the classroom has represented an exciting era at Albany Senior High School (ASHS). The Bring Your Own Device (BYOD) program builds on the positive developments that have provided a wealth of rich educational resources and tools, that when used effectively, can deliver very positive teaching and learning outcomes. However, if the implementation of this new technology is not properly controlled there are certain pitfalls that students may encounter.

The Department of Education supports students in the appropriate and safe use of their devices. By alerting parents and students to potential dangers, developing guidelines and providing advice and support, the exposure of students to potential problems can be minimised.

When the BYOD program commenced at ASHS in 2014 the school allowed students to bring either an Apple or Windows device to school. This has been challenging for school staff as there has been the need to learn to use two systems (Windows and Apple) to enable them to support students. For this reason the school has made the decision that from the beginning of 2017 students entering the BYOD program will be required to bring a **WINDOWS** device.

This document is specifically aimed at parents and students who are involved in the Albany Senior High School BYOD program and details the policy, guidelines and support strategies to ensure that students are able to make effective use of their devices and avoid any problems.

Appendix A, the BYOD Usage Agreement, needs to be returned with the device the student will be using. Technical staff will ensure the device meets the BYOD specifications, as outlined in this document and connect the device to the internet.

2 DESCRIPTION AND PURPOSE OF THE PROGRAM

Student owned devices will be permitted for use within the school for the express purposes of educational learning. Student devices will link to a campus-wide wireless network providing access to the internet and online curriculum materials. Under current school-wide guidelines, student owned devices are not permitted to access the school's network domain. This will require students to use external data storage devices, such as USB thumb drives or portable hard drives, online submission methods to transfer files to and from their devices, or cloud storage

Smart phones (defined as any mobile phone that is able to perform many of the functions of a computer; typically featuring a large display with touch-screen capability, network connectivity capability, camera and media handling features, file storage capability and an operating system capable of running applications) have proven to be useful tools providing a range of features and applications that can be used to complement and/or enhance the delivery of curriculum by teachers. Amendment to the school policy on smart phones allows for use of these devices by students only under the direction of teachers. Unauthorised use will remain in breach of school policy. Smart phones are not considered a BYOD device and will not have access to school systems, however students sometimes find them useful. Use of phones in class is governed by the Mobile Phone Policy and at the direction of the class teacher.

In cases where students are to use specific software or where subject requirements necessitate a need, the school currently maintains labs with computers setup for the express purpose of specialist courses such as Media, Business Education and Technical Graphics.

Whilst it is not the intention for the school to specify the type of devices that may be used under the program, we do specify that the device is a **WINDOWS** device and as a minimum should:

- Enable a student to easily read and input information (write and edit/manipulate text and graphics);
- Support Office productivity type applications that provide the following features: word processing, spreadsheets, slideshows and export files in formats that are supported by MS Office (e.g. .doc, .docx, .xls, .ppt, etc. It is important to note that as a student of Albany Senior High School the use of Office 365 is made available to students at no cost.
- Provide adequate battery life (including wireless network use) to operate for a school day.
- Provide an adequate screen resolution/view that minimises eye strain and fatigue when reading, whilst performing text entry, viewing media, etc.
- Supports the installation of anti-virus/anti-malware applications.

- Web browser support (e.g. Google Chrome, Mozilla Firefox, IE).
- Provides adequate ports to allow for peripheral attachment (e.g. USB thumb drives, portable Hard disk drives HDD, mice etc.)

Whilst this list is not exhaustive it should assist in the selection of an appropriate device for use in school. Further information is available in the BYOD Specification Guide which forms part of this document.

3 RESPONSIBILITIES

3.1 The Role of Students

Students must use their device and the school computer network responsibly. Communications on information networks are often public and general school rules for student behaviour, conduct and standards will apply. The misuse of ICT devices (including BYOD and school computers) is considered to be a behaviour management issue and will be dealt with within the existing school processes. It is essential that students follow the Usage Agreement (Attachment 1) included in this document and the Acceptable On-line Usage Agreement at all times.

It is highly recommended that students purchase a hard case and organise access to a locker at school to store their device when not required for practical subjects such as Physical Education and during breaks.

When using their device and accessing school information resources students must follow the guidelines detailed in this document.

Students who fail to honour this policy may forfeit the use of their device within the school and/or access to the school's wireless network.

3.2 The Role of Parents or Guardians

Parents or guardians are required to take responsibility for conveying the importance of the information included in this document and other school policies to their children. They are also required to monitor their child's use of their device to ensure that system updates, and anti-virus software updates are performed regularly. Parents or guardians are also to ensure that whilst the device is being used at school, their child understands that they must comply with school and Department of Education policies.

3.3 The Role of Teaching Staff

School teaching staff will monitor appropriate use of devices in accessing curriculum information. They will also provide guidance and instruction to students in the appropriate use of such resources.

This includes staff facilitating student access to information on their devices in support of and to enrich the curriculum while taking into account the varied instructional needs, learning styles, abilities and developmental levels of students.

School staff are not responsible for providing technical support for student owned devices brought to school.

3.4 The Role of the School

The school commits to upholding the BYOD Usage Policy and Guidelines, providing internet access to students in the BYOD program, and provide necessary resources to enable safe, educationally relevant access to the curriculum facilities for staff and students.

The school also has a responsibility to ensure that information published on the internet by students, or by the school (under the school's name) meets legal requirements and community standards in relation to intellectual copyright and safety.

4 GUIDELINES FOR PROPER CARE OF BYOD'S

4.1 Security, Transport and Storage

It is the responsibility of the student to ensure their device is stored in a safe and secure manner whilst it is used at school. It is recommended that a suitable protective case is used when transporting the device. Lockers are available and can be obtained for a minimal fee via application through the Accounts office.

4.2 Occupational Health and Safety Guidelines

The basic health and safety guidelines for desktop computers also apply to notebook use:

- Keep the upper arms relaxed at the side of the body.
- Bend the elbows to around 90 degrees.
- Keep the wrists straight.
- Change position every 15-20 minutes and take a complete break to get up and move your body every 30-60 minutes.
- If possible, a keyboard and mouse should be used at home.

Students with special needs will be catered for according to Department of Education guidelines.

4.3 Loss or Damage

Warranty repairs and insurance of devices brought to school under the BYOD program are not the responsibility of the school and will remain the responsibility of the child, parent or guardian.

Albany Senior High School takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices. In cases of theft or deliberate damage to devices brought to school, it remains the responsibility of the student or parent/guardian to report the incident to the school, for investigation under the school's Behaviour Management policy.

5 DATA MANAGEMENT

Saving or back-up of data is the student's responsibility. To back-up their work students will need to purchase a USB thumb drive, or alternatively an external hard drive. Under the school's and Education Department's BYOD agreement, access for BYOD devices is limited to the school's wireless internet. Access to school network drives will not be made available. This will, at times necessitate the need for students to transfer data stored on their devices to school computers using their USB flash drive or external hard drive.

Staff will not accept data loss as an excuse for not handing in work on time.

The student and their parents/guardians will be solely responsible and legally accountable for any data stored or installed on the student owned device.

6 PRINTING

Students will not be able to print from their BYOD device. In order to facilitate printing, it is essential students bring to school a USB thumb drive or portable hard drive.

Students should minimise printing at all times by print-previewing, editing on screen rather than on printouts and perform spell-checking before printing.

7 VIRUS PROTECTION

It is a requirement of this agreement that student-owned devices brought to school must have anti-virus software installed. This software is to be configured to perform regular updates and automatic scans for viruses/malware on the device. On the detection of a virus or the suspicion of a viral infection, the student must inform the school technician immediately. Anti-virus software is not available for installation from the school and is the responsibility of the parent or guardian. Devices without virus protection will not be allowed access to the school network.

8 ACCEPTABLE USE POLICIES AND CODE OF CONDUCT

The Acceptable Online Use Agreement and the BYOD Usage Agreement are written agreements that formally set out the rules of use of software, networks, printers, emails, online teaching and learning, files storage and sharing, internet and access to DoE Portal from home if you have access to the internet. All staff and students accessing Department of Education Systems and are bound by Department of Education rules of use.

Computer operating systems and other software installed on the device must comply with the minimum requirements set by the school and the Education department to maximise the usefulness of the device. Students are prohibited from:

- Bringing or downloading unauthorised programs, including games, to the school or running them on their devices or on school computers. Online internet games are banned.
- Break software copyright. Copyright is to be observed at all times. It is illegal to copy or distribute school software. Illegal software from other sources is not to be copied to or installed on devices used in the school or on school equipment.
- Deliberately introduce any virus or program that reduces system security or effectiveness.
- Attempting to log into the network with any user name or password that is not their own, or change any other person's password.
- Revealing their network password to anyone except the system administrator. Students are responsible for everything done using their accounts and everything on their notebooks. Since passwords must be kept secret, no user may claim that another person did anything to cause school rules to be broken.
- Using or possessing any program designed to reduce network security.
- Enter any other person's file directory or do anything whatsoever to any other person's files.
- Attempting to alter any person's access rights; or
- Storing the following types of files on their device or school computer, without permission from their teacher:
 - Program files.
 - Compressed files.
 - Picture files, unless they are required by a subject.
 - Obscene material – pictures or text.
 - Obscene filenames.
 - Insulting material.
 - Password-protected files.
 - Copyrighted material.

8.1 Access Security

It is a condition of the BYOD program that students agree to the monitoring of all activities including their files, e-mail and Internet accesses whilst connected to the school's network.

8.2 Monitoring and Logging

A log of all access to the internet including e-mail will be maintained and periodically scanned to ensure that undesirable internet sites have not been accessed and that the content of e-mail remains within the guidelines described in this document.

8.3 Internet usage

Internet access is expensive and has been provided to assist students' education. Students must use it only with permission, and not in any unauthorised way.

As the Internet is an unsupervised environment, the school has a responsibility to ensure that, as far as possible, material obtained from the Internet is not offensive or inappropriate. To this end, filtering software has been placed on the Internet links. It is the responsibility of individual students to ensure their behaviour does not contravene school rules or rules imposed by parents/guardians.

The school is aware that definitions of "offensive" and "inappropriate" will vary considerably between cultures and individuals. The school is also aware that no security system is perfect and that there is always the possibility of inappropriate material, intentionally and unintentionally, being obtained and displayed.

It is the responsibility of the school to:

- Provide training on the use of the Internet and make that training available to everyone authorised to use the school's internet link.
- Take action to block the further display of offensive or inappropriate material that has appeared on the internet links.

Students must not deliberately enter or remain in any site that has any of the following content:

- Nudity, obscene language or discussion intended to provoke a sexual response.
- Violence.
- Information about committing any crime.
- Information about making or using weapons, booby traps, dangerous practical jokes or "revenge" activities.

Students must:

- Follow school guidelines and procedures when preparing materials for publication on the web.
- Not use material from other web sites unless they have permission from the person who created the material. If unsure, they should check with their teacher.
- Not access any other material that their parents or guardians have forbidden them to see. If students encounter any such site, they must immediately turn off the notebook and notify a teacher. They should not show the site to their friends first.
- Ensure that their use of sites such as "YouTube" is integral to their course- not for recreational use.
- Ensure that Facebook and other social media sites are not accessed during class and break time.
- Understand that use of sites that contain video, music and games slow the network down and thus should only be used to complete set tasks.

8.3.1 Chat lines and instant messaging (IRC, mIRC, SnapChat, Viber, WhatsApp etc)

Unless instructed by a teacher real-time chat programs and instant messaging services such as Snap Chat, Facebook, Twitter, Messenger, Reddit, etc. are not to be used by student.

8.3.2 Cyber safety

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 sites online for further useful information:

The main government cyber safety information website at <http://www.cybersmart.gov.au/>

Cybernetrix page on the internet: <http://www.cybersmart.gov.au/cybernetrix/index.html> Internet Safety for Secondary Students section.

- **ALL** students (and their parents) with a BYOD must complete a **Usage Agreement Form**. These can be collected from the **school front office** or downloaded from our school website; the form needs to be returned to the **school front office** before your BYOD device is used at school. On registration approval **ALL** devices will be **identified by a tamper proof sticker** applied by school IT technicians.

Hardware Requirements

Form Factor	Laptop or convertible device. A convertible device must have a physical keyboard available (with full QWERTY keyboard layout).
Physical Dimensions	Minimum Screen Size: 9", maximum screen size 15.6"
Wireless Compatibility	Wireless connectivity required. Minimum specifications: 802.11 a/b/g 2.4Ghz
Battery Life	Minimum: Advertised battery life of 5 hours or more. <i>NOTE: It is a requirement for the battery to be fully charged at home in preparation for the following school day.</i>
Storage	Minimum: <ul style="list-style-type: none"> • 160GB HDD (Hard Disk Drive), or • 32GB storage on device (Solid State Drive) Note: Students are recommended to make use of an external storage device such as a USB thumb drive, USB portable hard drive, and/or Cloud storage (e.g. Google Drive) to back up their work.
Protective casing	Students are required to store their device in a suitable protective case when not being used.
Additional Recommendations	<ul style="list-style-type: none"> • USB 2.0 or USB 3.0 ports • Accidental loss and breakage insurance

*NOTE: Hardware repair and hardware/software faults remain the responsibility of the device owner.
The owner accepts all responsibilities for the use of the device whilst at the school.*

Software Requirements

In addition to the hardware requirements outlined above, the device must also have access to the following software.

Operating System	Microsoft Windows 10 or Windows 10 Pro* . No other OS are supported (e.g. MacOS, Chrome, Ubuntu, etc.) <i>*Highly recommended – Operating System technical support can be provided for BYOD devices that are joined to school network using the professional version of Windows 10.</i> NOTE: Software and hardware support always remains the responsibility of device owner.
Web Browser	Internet Explorer/Edge, Mozilla Firefox and/or Google Chrome
Word Processing; Spread sheets & Presentation	Microsoft Office. Please Note: Microsoft Office 365 is supplied free of charge for students via Department of Education – please see our Technical staff for information on downloading.
PDF Document Viewing Software	Adobe Acrobat Reader (free download).

Students should ensure that they bring a thumb drive or portable hard drive (HDD) and ensure their device is fully charged each day. Access to readily available power supplies is limited within classrooms.



ALBANY SENIOR HIGH SCHOOL BYOD User Agreement

Key points of the BYOD Usage Policy are noted below:

1. The student will abide by all conditions outlined in the Students Online – Acceptable Usage Policy.
2. The student and their parent will be solely responsible and legally accountable for any data stored or installed on the student owned device.
3. The student must bring their thumb drive, hard case and fully charged device to school each day. NB: students need to monitor battery use to ensure that the computer will be functional for the day.
4. The student must take all reasonable care to prevent against any form of damage and loss of the student owned device.
5. The student is responsible for the safe storage and care of their device *at all times*. During Phys Ed and other practical subjects when not needed they are to be placed in lockers prior to the lesson beginning. Lockers must be used during breaks.
6. It is strongly recommended that:
 - a. Student owned devices are installed with Anti-Virus protection which is either current or the version immediately prior to the current version:
 - b. Student owned devices are installed with the recent release of the anti-virus definitions files (one of the most recent four (4) released definitions).
 - c. Student owned devices have Operating System patches which are within seven (7) days of the vendor's release date.
 - d. Student owned devices are enabled to receive auto-updates from the software vendor.
7. The student owned device and any software installed will be provided by the Parent and or Student.
8. Student owned devices can only be connected to the school's wireless network.

----- ✂ -----

ALBANY SENIOR HIGH SCHOOL BYOD Usage Agreement

I have discussed the implications and rules of BYOD devices being used in the school with my son/daughter. We agree to adhere to the Albany Senior High School and the Department of Education BYOD Usage Agreement and Acceptable Online Usage Agreement Policy and Guidelines. I give permission for my son/daughter to bring their device to school each day ensuring that it is fully charged and that system and virus protection updates are performed regularly in compliance with the BYOD Usage Policy and Guidelines.

Student's Name _____ **Year level** _____

Student Signature _____ **Date** _____

Parent/Guardian Name _____

Parent/Guardian Signature _____ **Date** _____