Duncraig Senior High School

Bring Your Own Device

Computer Usage Policy Information

for Parents and Students

Table of Contents

1 INTRODUCTION

The integration of 'Bring Your Own Device' (BYOD) and supporting information technology equipment into the classroom represents an exciting era at Duncraig Senior High School. The BYOD project provides 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.

Duncraig SHS supports students in the appropriate and safe use of their BYODs. 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.

This document is specifically aimed at parents and students who are involved in the "Duncraig Senior High School Bring Your Own Device Project" and details the policy, guidelines and support strategies to ensure that students are able to make effective use of their BYOD and avoid any problems.

2 DESCRIPTION AND PURPOSE OF THE PROJECT

The objective of the BYOD project is to implement a range of innovations that explore and exploit the latest in educational technology in a sustainable program. Duncraig sees the value of one to one computer devices in teaching and learning and would like to have it available to all student.

BYOD will link to a campus wide wireless network providing access to the internet and curriculum materials as well as enabling communication between students and teachers.

Teachers have been issued with their own device and have participated in a range of professional learning programs to develop teaching and learning strategies to value add using the device. Students' engagement and productivity is enhanced with their own BYOD as many of their learning resources are on the device and improved communication with their teachers with the ability to electronically connect to them at any time.

We request parents supply a device that complies with the following specifications:

- ***Apple*** device with at least --- 10 inch screen, 10 hour battery life and running OSX 10.8 or above or IOS 6.4 or above ***OR***
- ***Windows 10*** device with at least --- 10 inch screen, 10 hour battery life and running version Windows 10 or above.
- ***Software/Apps installed –*** Students will be able to install Office 365 to their BYO Device when they are attending school:
    - PDF markup – e.g. Preview or Adobe Reader
    - Cloud storage – e.g. Dropbox or Google Drive or Copy
    - Image editing – e.g. iPhoto or Photo Gallery or Photoshop
    - Video editing – e.g. iMovie or Movie Maker
    - Web browser – e.g. Safari or Chrome or Firefox or Internet Explorer
    - Online accounts (e.g. Evernote, Dropbox, Google Drive, etc) can be created privately or at school with the students education email account (first.last@student.education.wa.edu.au)
- ***BYO Device agreement*** signed and returned.

There is a wide range of devices on the market (It will be your choice which model you choose as long as it complies with the specifications above). DSHS is offering a range of devices in a bundle including support, cover and App credit through Winthrop Computing https://portal.winaust.com.au/a/duncraigshs. (Login 4129). There is also the option to purchase insurance with the device or lease a device over 2 or 3 years with insurance included. These options will be at extra cost. There is no obligation to purchase the device through Winthrop. You may already own one or prefer to organize your own through another vendor. Note: if your child has their own device they will be able to bring that at their own risk. We would recommend personal insurance.

Duncraig will be improving communication with parents by opening a parent portal. Our web portal will give you access to information whenever you want, on any device you are using. You can view your child's assessment requirements, attendance, school notices and a wealth of other important information.

3 RESPONSIBILITIES

3.1 The Role of Students

Students must use their BYOD 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.

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

Students who fail to honour this Code of Conduct may forfeit use of their BYOD and access to the Internet and/or school network.

3.2 The Role of Parents or Guardians

Parents or guardians are required to take responsibility for conveying the importance of the policy guidelines in this document and other school policies to their children. They are also required to monitor their child's use of the BYOD, especially at home, including access to media and information sources.

3.3 The Role of Teaching Staff

School teaching staff will monitor appropriate care of the BYOD and its use 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 BYOD in support of and to enrich the curriculum while taking into account the varied instructional needs, learning styles, abilities and developmental levels of students.

3.4 The Role of the School

The school commits to upholding the Usage Policy Guidelines and providing physical and financial resources to enable safe, educationally relevant access to the BYOD and relevant curriculum facilities for staff and students.

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

4 AUTHORISATION AND RULES FOR HOME USE

Students will be expected to bring their BYOD to school to use in class. This will be subject to approval by Parents/Guardians as indicated on the School Usage Permission Letter and also by student compliance with the usage conditions outlined in this document.

School usage will be granted subject to adherence to the following rules:

1. Students must bring their BYOD to school each day. **It must be fully charged**.
2. The Students must have their BYOD inside their protective cover and inside their school bag when travelling to and from school.
3. Students are responsible for the safe storage and care of their BYOD AT ALL TIMES. For example BYODs should not be left outside classrooms or the library.
4. When the BYOD is at school the school Network Agreement applies at all times.

Since school use brings with it a risk of accidental damage or theft of the BYOD we expect parents to arrange insurance. If an insurance claim is partially or wholly rejected by the insurer due to non-compliance with the guidelines the school will not cover the cost associated with the loss or damage.

5 GUIDELINES FOR PROPER CARE OF BYOD

5.1 Security and Storage

When the BYOD is at school, students must know the location of their BYOD at all times and are responsible for ensuring its safe keeping. When the computer is not required in class, for example during Physical Education, it is to be placed in the secure storage provided. BYODs must also be under the student's direct care during recess and lunchtime.

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

5.2 Transport and Handling Procedures

When transporting the BYOD, students are to make sure that it is in the cover and in their school bag which must be securely closed. Students must carry their BYOD inside the cover and place this inside their school bag when leaving the school. Students must never remove the BYOD from its cover and place it directly into their school bag.

5.3 Occupational Health and Safety Guidelines

The 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 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.

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

5.4 General Care of the BYOD

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

5.5 Report of Loss or Damage

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

6 DATA MANAGEMENT

Saving or back-up of data is the student's responsibility. To backup work it is recommend that students use cloud storage, purchase a USB flash drive or preferably, an external hard drive.

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

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

Students will have limited access to network printers. Printing will be supervised by the teacher in charge of the learning area in which the student wishes to print materials. Students must arrange for this to be conducted during class time or at another time convenient for the classroom teacher.

8 VIRUS PROTECTION

The BYODs should be configured with anti-virus software which regularly and automatically checks for viruses on the device. On the detection of a virus or the suspicion of a viral infection, the student must inform the Network Administrator, Mr John Cregan.

9 ACCEPTABLE USE POLICIES

Any Acceptable Use Policy is a written agreement that formally sets out the rules of use of software, networks, printers and the Internet. All staff and students are accessing the Department of Education System and are bound by Department of Education rules of use.

Computer operating systems and other software have been set up to maximise the effectiveness of the BYOD. Students are prohibited from:

- Bringing or downloading unauthorised programs, including games, to the school or running them on school computers.
- Online internet games are banned.
- Accessing social media sites eg. Facebook at school is banned.
- Deleting, adding or altering any configuration files.
- Breaking 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 the school equipment.
- Deliberately introducing 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 network administrator. Students are responsible for everything done using their accounts and everything on their BYOD. Since passwords must be kept secret, no user may claim that another person entered their home directory and 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 in their home directory, 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.

9.1 Access Security

It is a condition of entry to the BYOD for Students Project that students agree to the monitoring of all activities including their files, e-mail and Internet accesses.

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.

9.2 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. Ultimately, 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 websites 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 BYOD and notify a teacher. They should not show the site to their friends first.

9.2.1 Chat lines (IRC, MIRC, ICQ etc)

Real-time chat programs (MIRC, ICQ) are not to be used by students unless instructed by a teacher.

9.2.2 Cybersafety

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:

http://www.cybersmart.gov.au/ ------ Federal Government cybersafety information website

www.cybernetrix.com.au --- Internet Safety for Secondary Students