Karratha Senior High School

Bring Your Own Device

Computer Usage Policy

Table of Contents

1 INTRODUCTION

The integration of 'Bring Your Own Device' (BYOD) and supporting information technology equipment into the BYOD refers to students bringing a personally owned device to school for the purpose of learning. In 2020 Karratha Senior High School (KSHS) will be moving to this model for all Year 7, 8, 11 and 12 students with the option for Yr. 9 -10 to engage in the program, allowing them to bring a personal laptop to school for educational purposes. KSHS recognises the need to prepare students for a rapidly changing world where technology plays an increasing role in students' everyday lives.

This document is specifically aimed at parents and students who are involved in the "KSHS Bring Your Own Device Program" 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 BYOD

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.

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

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

- ***Windows 10*** device with at least –
  - 10 inch screen
  - 4GB RAM
  - 128 GB Hard Drive
  - 10 hour battery life
  - running Windows 10 or Windows 10 Pro or Windows 10 S.
- ***Software/Apps installed –*** BYO devices must have these software/apps installed for the teaching and learning program at Karratha SHS:
  - Note taking – e.g. Evernote or Onenote
  - PDF markup – e.g. Preview or Adobe Reader
  - Word processing – e.g. Word
  - Spreadsheet – e.g. Excel
  - Presentation – e.g. Powerpoint
  - Image editing – e.g. Photo Gallery or Photoshop
  - Video editing – e.g. Movie Maker
  - Web browser – e.g. Chrome, Firefox or Internet Explorer
  - Online accounts (e.g. Evernote, Google Drive, etc) can be created at home or at school with the students education email account (first.last@student.education.wa.edu.au)
- ***A 'School' profile is created on the laptop –*** this profile will be configured to the KSHS network. The password for this profile must be provided to the ICT Administrator or any staff member upon request.
- ***BYOD 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). You may already own one or prefer to organize your own through your preferred 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.

KSHS communicates regularly with parents through the Department of Education (DoE) parent portal 'Connect' at https://connect.det.wa.edu.au/. This 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 the Karratha SHS Code of Conduct, school rules for student behaviour, and Karratha Acceptable use of ICT Policy will apply at all times.

Any material stored on the BYOD under any profile and accessed at school is subject to the DoE and KSHS Acceptable use of ICT Policies, KSHS Code of Conduct and KSHS BYOD Policy.

Students are to only use their BYOD under teacher instruction.

Students are only to use their BYOD in a classroom environment. Use at recess and lunch is only allowed under teacher supervision.

Students may not use 'hotspot' networks via mobile devices at school to access the internet.

Students BYOD must be fully charged each day. Charging facilities will not be available during the day.

Students who fail to honour the BYOD Policy 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 and materials stored on the device.

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 resources to enable safe, educationally relevant network access to the BYOD and relevant curriculum facilities for staff and students.

KSHS has a responsibility to ensure that, as far as possible, material obtained from the Internet is not offensive or inappropriate. To this end, DoE software will filter and monitor internet sites and usage whilst the BYOD is connected to the KSHS network.

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 GUIDELINES FOR PROPER CARE OF BYOD

4.1 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. BYODs must 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 (e.g. in a vehicle). In these circumstances, the BYOD can become a target for theft.

4.2 Transport and Handling Procedures

When transporting the BYOD, students are to make sure that it is in a protective cover and in their school bag or laptop bag/backpack which must be securely closed. Students are not to walk around the school with the BYOD open or in hand.

4.3 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 DoE guidelines.

4.4 General Care of the BYOD

It is the student's responsibility to maintain the BYOD in good condition. KSHS takes no responsibility for damage or theft of the BYOD.

4.5 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.

4.6 Insurance

Since school use brings with it a risk of accidental damage or theft of the BYOD, we expect parents/carers to arrange insurance. KSHS takes no responsibility for damage, loss or theft of any BYOD device.

5 DATA MANAGEMENT

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

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

6 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, preferably through the Connect classroom.

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 no access to network printers. Printing will only be available from KSHS school managed computers.

7 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 their Deputy Principal to notify the Network Administrator.

8 ICT 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 DoE Network are bound by DoE 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 e.g. Facebook, Instagram, Snapchat at school is banned.
- Streaming media of any type 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 username 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 or accessing any website designed to reduce network security e.g. proxy bypass.
- 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 Laptop:
    - Obscene material – pictures or text
    - Obscene filenames
    - Insulting/offensive material
    - Copyrighted material.

8.1 Access Security

It is a condition of entry to the BYOD program 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.

8.2 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. Bandwidth is limited at KSHS to 20Gb/s and as such, students may experience longer than normal times for access to certain web pages depending on the network traffic at the school.

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.

KSHS will take action to block the further display of offensive or inappropriate material that has been accessed through the network as it is identified.

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.

8.2.1 Chat lines

Real-time chat programs are not to be used by students unless instructed by a teacher.

8.2.2 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

9 USER AGREEMENT

STUDENT PARENT MEMORANDUM OF AGREEMENT

Connection and Use of Student Owned Device on the Karratha SHS Network.

Student's Full Name:_____Parent/Carer Full Name :_____

Device Make/Model: _____

Preamble

This memorandum relates to the connection and use of a student owned device at Karratha SHS. This memorandum describes the terms of the provisions including level of service and scope of services agreed to by Karratha SHS, the student and the student's parent(s)/carer(s).

Conditions

The network is supplied by Karratha SHS to the student, based upon the following Agreement:

1. The student will abide by all conditions outlined in the DoE and KSHS Acceptable Usage of ICT Policy and BYOD Policy.
2. Students must create a 'School' profile on their device and provide the password for this profile to the ICT Administrator or any staff member upon request. The 'School' profile is the only profile allowed access to the KSHS network.
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 owned device and any software installed, will be provided and maintained by the Parent and or Student.
4. Student owned devices can only be connected to the school's wireless network.
5. The DoE strongly recommends 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.*

Signed: _____ Date: _____

Student's Full Name: _____

Signed: _____ Date: _____

Parent/Carer Full Name: _____

Laptop School Account User Name: _____

Laptop School Account Password: _____

Connect Username:_____

Connect Password:_____