KINROSS WOLAROI SCHOOL

ICT Acceptable Use Policy

Revised September 2017

This Policy applies to all who use the KWS ICT Systems and Network

To acknowledge this policy, send an email to support@kws.nsw.edu.au stating that you *have read and accept the terms of the ICT AUP*

September 2017

Contents

Introduction 3
General Policy Overview (compliance guideline) 3
Computer Hardware and Software 4
Kinross Wolaroi School Computer Network Access and Use 4
Information Security and Privacy (applies to VISITORS and STAFF) 5
Password Management 6
Computer and Network Use 7
Use of Personal Devices on the School Network (BYOD) 7
Printing 8
Email 8
Internet Access and Usage 9
World Wide Web 9
Acceptable Social Media 10
Unacceptable Social Media 10
Proxies 10
Torrents 11
Related Policies or documents 11

Introduction

The Kinross Wolaroi School ICT environment is provided for staff, students and visitors to help enable teaching and learning.

Staff and students are given access to the data network with an individual account allowing Internet access. Access to the Internet is filtered and monitored. Usage is recorded for each individual account. These facilities should be regarded as a privilege which may be withdrawn if misused.

General Policy Overview (compliance guideline)

1. Use of computer/internet resources for educational purposes has priority over all other uses.
2. Recreational use is allowed during certain times for Boarding students and Resident staff
3. Individuals are expected to use the school ICT resources in a responsible and considerate manner. Each individual will be held responsible and accountable for their actions
4. Appropriate language is expected in all communication, including electronic communication. Inappropriate content, words or phrases may be captured by the internet filter and highlighted to the Principal, or Principal's delegate
5. No individual may deliberately or carelessly waste or damage computer resources (e.g. unnecessary printing) or disadvantage other users e.g. by monopolising or compromising equipment, network traffic etc.
6. Consideration must be given to assure convenience to others. For example:
    - use headphones to listen to sound or music
    - log-out and leave computer ready for the next user to log in
    - do not leave programs running on computers when you leave
    - clean up any mess and not leave rubbish or paper lying around computers
    - replace furniture to normal positions when you leave
    - shut down or power-off the computer if you are in the last period of the day
7. Information Security and Privacy is important from a personal and school wide perspective. An individual may access information on a need-to-know basis and may not share information outside the area of its intended use.
    - It is considered to be a breach of Information Security if information that is not relevant to an individual's area of responsibility is encountered
        - Such information is to be ignored and not referred to in future
        - Each instance of Information Security breach is to be reported to the Director Information Services

Computer Hardware and Software

Computer facilities are expensive and care must to be taken to ensure availability for all. It is important computer equipment is treated with respect and care. Individuals must not:

- Do anything likely to cause damage to equipment, whether deliberately or carelessly, including (but not limited to):
    - Steal, damage, deface any equipment
    - Interfere with networking equipment such as Access Points, switches, hubs and network cables

Individuals must not, without permission from Director Information Services:

- Attempt to repair equipment
- Unplug cables or move equipment
- Remove any covers or panels or disassemble any equipment
- Disable the operation of any equipment

Computer operating systems and other software must be set up properly for computers to be useful. Staff, Students and visitors must not:

- Change computer settings (including screen savers, wallpapers, desktops, menus, standard document settings etc.) without permission
- Bring or download unauthorised programs, including games, to the school or run them on school computers. **Online internet games are blocked during school hours. For boarders, the Head of House (or delegate) has discretion to allow on-line internet games.**
- Copy any copyrighted software to or from any computer, or duplicate such software without licence to do so.
- Format shift digital content (video/audio/other), unless in accordance with Copyright law

Kinross Wolaroi School Computer Network Access and Use

Network accounts are to be used only by the authorised owner of the account. If you find a computer logged in, you should log that user out and restart the computer and do nothing else within that person's account. It is the responsibility of staff and students to make backup copies of their work. The school will exercise due care with backups but will not be held responsible for lost data.

Throughout the school year staff and students will be responsible to keep their folders on the network in a clean, organised, uncluttered manner. At the end of Year 6 and Year 12, student content will be removed. Consequently students have a responsibility to take a copy of their work before the end of Year 6 and Year 12. It is important individuals are responsible and frugal with the use of network storage.

It is very important if you are part of the iPad program to ensure you back-up the educational data that is on your iPad. This may be achieved by backing up to the iCloud, or a personal computer or Laptop.

Information Security and Privacy (applies to VISITORS and STAFF)

The security and privacy of information is important. Individuals have differing access to information depending on their role within the organisation.

Information Security and Privacy is important from a personal and school wide perspective. An individual may access information on a need-to-know basis only and may not share information outside the area of its intended use.

- It is considered to be a breach of Information Security if information that is not relevant to an individual's area of responsibility is encountered.
- Such information is to be ignored and not referred to in future.
- Each instance of Information Security breach is to be reported to the Director Information Services

Publication of information in any form identifying KWS students or its employees must be performed with care and must be in accordance with KWS Privacy Policy (refer KWS website). Posting to social media needs to be in accordance with the KWS Staff Code of Conduct and aligned with KWS Social Media Policy (refer KWS Website).

Password Management

1. The Network Administrator, in consultation with the school's ICT Learning Integrator(s), shall guide all staff, secondary students and visitors to comply with the following password management principles:

Password attribute	Suggested Minimum Standard year 5-12 and staff
Length of password	At least 8 characters
Password complexity – Mix of Characters	At least one Capital letter; at least one lower case; at least one number or at least one symbol (,.!@#$%^&*)
Number of unsuccessful login attempts before the Account is locked out	10 attempts for students 5 attempts for staff
Duration of lockout period	30 minutes – or notify the Network Administrator to reset the password
Period after which a password must be changed	180 days (every 6 months) - Users also have the ability to change their own passwords at any time
Reusability of old passwords	A password that has been used before cannot be used again

2. A person issued with a password has a responsibility to change it immediately after he/she:
    a. Has been issued with the initial default password
    b. Has used the same password for more than six months
    c. Is advised by ICT staff to change it
    d. Has reason to suspect the password has been observed or compromised

3. A person must not:
    a. Share the password with anyone
    b. Write the password down in an insecure location
    c. Ask another user for their password for ANY reason. If access to their files is required then a written request to the KWS Network Administrator is required

4. A breach of points 2 or 3 of this policy may result in the suspension of the user account.

5. In the case of K-4 students, each student password will be recorded in a secure location by their classroom teacher and accessed wherever it is needed. In these situations, small cards may be produced to help K-4 students with the use of their username and passwords. The classroom teacher is required to destroy this information when the student leaves that teacher's class.

Computer and Network Use

Individuals must not:

- Attempt to log into the network with any user name or password that is not their own, or change any other person's password
- Reveal their password to anyone except the Network Administrator. The only exception is Prep School students who may reveal their password to classroom teachers
- Use or possess any program designed to reduce network security. Refer to **Use of Proxies** section on the next page
- Enter any other person's home directory or do anything whatsoever to any other person's files
- Attempt to alter any person's access rights, including their own
- Store the following types of files in their home directory, without permission from the Director Information Services:
    - Program files (EXE, COM, BIN etc.)
    - Music, Picture and Video files, unless they are specifically required by a subject and **do not breach copyright law**
    - Inappropriate material – pictures or text including inappropriate filenames
    - Material in breach of Copyright

Use of Personal Devices on the School Network (BYOD)

With an increasing number of staff, students and visitors using their own computers on the school's network, it has become necessary to outline the requirements for Bring Your Own Device (BYOD).

1. The school has an iPad program for years 5-9. This is not considered BYOD
2. BYOD are allowed in the Boarding House for Homework and recreational purposes. At this stage no BYODs are allowed to be used in the classroom
3. Personal devices must have the Schools Anti-Virus software installed as a pre-requisite to connecting to the school network. This helps to ensure the safety of their files and the school's network. The Network Administrator and Network Technician will be available to advise, guide and assist.
4. Many devices: (laptops, iPads, tablets, phones) come standard with wireless access cards and hardware. Publicly available internet providers such as Bigpond or Optus **will not** necessarily have the security or filtering software that is available via the school's network. In such cases, the school will not take responsibility for any material that is accessed and stored on those devices. This outside Internet access entails extra expense for students and parents.
5. Some programs allow the sharing of audio and video files.
    a. The sharing of music files across the school's network raises serious copyright issues for both the school and the students involved and therefore the sharing of files is not condoned by the school and not permitted

   b. The sharing of video content is allowable via the Schools DVC or commander system. Sharing video content by other means could result in copyright breach

6. BYOD devices must not have a bridge configured between its Network adapters
7. Connection to the school's wireless network is granted once the computer details are provided to the school's Network Administrator. Specifically, the person's name, computer name and the MAC address must be provided

Printing

KWS has a Follow-me printing model. A Print job may be sent toi the Print_And-Follow queue and released from any Printer in the school. In the interests of our environment, the use of printing is to be minimised by: print previewing, editing on screen and spell-checking before printing.

Students must not load paper into printers without permission.

Paper that is pre-used, torn, creased, damp, irregularly shaped or sized should never be used in any printer, laser or ink jet.

Any damage resulting from inappropriate use may be charged to the account of the person responsible.

Students receive an allocation of $40 per term for printing. Any unused amount is not rolled over to the next term. Printing costs are as follows: 10c/page for A4 mono; 45c for A3 mono; 25c for A4Colour; and, 60c/page for A3 colour.

Staff and Senior School students are issued with a PhotoID card that serves as a Print Release card and has a barcode to allow borrowing from the school Library. This card may also provide the ability to make cashless purchases at the KWS Canteen and cashless travel on the late buses.

Email

Electronic mail is a valuable tool for personal and official communication both within the school's network and on the Internet. KWS is the owner of all emails created from KWS email accounts.

Staff must use their school email for all school related matters including (but not limited to) contact with: parents; peers; professional associations; others for the purposes of improving educational outcomes for students. Staff members are able to access other email services for private (non-school) matters on a limited basis in their own time. School related email communication is a priority. Students are restricted to school provided email.

Some tips for good use of email:

- Use appropriate language and be polite in your messages. Do not be insulting, abusive, swear or use vulgarities.
- Never write hate mail, chain letters, harassment, discriminatory remarks and other antisocial communication. No message should contain obscene comments, threats, sexually explicit material or expressions of bigotry or hate.
- Do not reveal your personal home address or the phone numbers of staff or students without consent

Note: email is **not private**. KWS is the owner of emails created in the schools environment. With permission from the Principal, a senior member of the ICT team may access all files including mail. Messages relating to illegal or inappropriate activities may be reported.

Individuals will not:

- send offensive or inappropriate email
- send email with large attachments, any mail with attachment >20MB is blocked
- send unsolicited mail to multiple recipients ("spam")

Internet Access and Usage

Internet access is expensive and has been provided to assist students' education. Students must use it in an appropriate and unauthorised manner. It is not intended for entertainment, except for boarding students during their downtime when authorised by the Head of House (or delegate).

Since 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 school's network so that it monitors and records details about Internet usage. All web access by students is tracked and logs are kept for a period of time.

Students who utilise more than their fair share of Internet data/bandwidth may have their Internet Accounts throttled back to a slower speed. 30G for Boarders and Resident staff, 20G for day students

This allowance is reset each month. A student or Resident staff may elect to renew their quota by agreeing to an additional charge on their account. The charge for internet quota top-up is $10 for each occurrence.

World Wide Web

The World Wide Web is a vast source of material of all sorts of quality and media. The school will exercise care in protecting students from inappropriate material, but the final responsibility rests with students in not actively seeking out such material. It is conceivable that, especially for senior students,

information is required for curriculum purposes that may appear to contravene the following conditions, i.e. some sites may be blocked by the internet filter when required for learning. **In such cases, it is the responsibility of students and teachers to request access to the KWS Network Administrator the need to access such sites.**

Students will not deliberately enter or remain in any site that has any of the following content (without permission from their teacher):

- Nudity, obscene language or sexual discussion intended to provoke a sexual response
- Gambling
- Dating
- Social media during school hours without approval
- Violence or racism or discrimination against minority groups
- Information on, or encouragement to commit any crime
- Any other inappropriate content

The only exception is if it forms part of an approved classroom lesson and is supervised by the teacher. If students encounter any such site, they must immediately turn off the computer monitor (not the computer itself) and notify a teacher.

Acceptable Social Media

Access to social media such as: Podcasts, WiKi's, Blogs, content communities (YouTube) are permitted if it is for educational use. Boarding students have limited access to social networking sites and the activity on these sites is filtered and monitored.

Unacceptable Social Media

The following types of social media are not permitted for day students unless there is an educational reason:

- virtual game worlds
- On-line gaming
- Social networking (Twitter, Tumblr, Facebook, Instagram and MySpace) other Social Networking

The following types of social media are not permitted for any students unless there is an educational reason: SnapChat, dating sites, anything deemed inappropriate by the Principal (or delegate).

Proxies

The use of proxy servers (proxies) or similar methods to bypass the school's content filtering software is considered a **breach** of the ICT AUP and as such will result in the immediate removal of the student's network **and internet access**. This applies to ALL students whether they are in Year 1 or

Year 12. This can and will affect the student's ability to complete set work including assessment tasks that are dependent on internet access. It is therefore up to the student to remain responsible and accountable for their actions. Letters stating this breach will be sent home to the student's parent or guardian.

Torrents

Torrents are used to enable downloading, distributing and sharing large amounts of data over the internet. Use of torrents is not permitted on the KWS Network.

Related Policies or documents

KWS Privacy Policy, refer KWS Website
KWS Social Media Policy, refer KWS Website
KWS iPad Program, refer KWS website