Ku-ring-gai High School

inspire challenge create

STUDENT ACCEPTABLE USE OF TECHNOLOGY AGREEMENT

The Student Acceptable Use of Technology Agreement incorporates the use of all digital devices (e.g. Desktop computers, laptops, tablets, printers, electronic equipment etc.) The school provides access and the use of these technologies with the expectation that students will make good decisions with regard to using it.

This Student Acceptable Use of Technology Agreement must be agreed to and signed before students are permitted to use any school device.

Students and parents/caregivers must carefully read this Agreement prior to signing it. Any questions should be addressed to the school and clarification obtained before the Agreement is signed.

This Agreement applies to the duration of your enrolment at Ku-ring-gai High School.

Student Acceptable Use of Technology Agreement

Agreement:

i. We have read the Student Acceptable Use of Technology Agreement.

ii. We understand our responsibilities regarding the use of all technologies and the Internet, including Section 3.1 Damage or loss of equipment.

iii. In signing below, we understand and agree to the Student Acceptable Use of Technology Agreement.

iv. We understand that failure to comply with the Student Acceptable Use of Technology Agreement will invoke the school's standard discipline procedures and/or the actions outlined in clause (5).

Name of student: ..... Year .....

Signature of student: ..... Date: ..... / ..... / .....

Name of parent/caregiver: .....

Signature of parent/caregiver: ..... Date: ..... / ..... / .....

PLEASE SIGN AND RETURN THIS PAGE TO THE SCHOOL

'Student Acceptable Use of Technology: User Agreement

1 Purpose

Ku-ring-gai High School Student Acceptable Use of Technology policy allows students to use digital devices and provides internet services in order to support their educational needs. Ku-ring-gai High School acknowledges that it has a responsibility to provide safe and secure online services. These digital devices and services are educational tools and must be used in a responsible manner. This policy recognises that there are constant advances and changes in the use of technology (e.g. software, apps, information sharing, social media platforms, new devices etc.). Therefore, students must seek advice and clarification from the school as soon as possible when engaging with new or unfamiliar technology.
Students and parents/caregivers must be aware of and consent to the conditions of this Agreement.

2 Scope and Definitions

2.1 Parties

This Agreement is between Ku-ring-gai High School, a student currently attending or who will be attending Ku-ring-gai High School, and their parent or caregiver.

2.2 "Student" and "Students"

Reference in this Agreement to Student or Students means a student currently attending or who will be attending Ku-ring-gai High School and binds their parent or caregiver.

2.3 "Student Acceptable Use of Technology Agreement"

This Agreement may be referred to as the Student Acceptable Use of Technology Agreement or User Technology Agreement.

2.4 "Device or Technology"

Reference in this Agreement to Device or Technology means an electronic device or equipment at Ku-ring-gai High School pursuant to the school's Student Acceptable Use of Technology Agreement

2.5 "E-Learning Account"

Reference in this Agreement to E-Learning Account refers to students' DEC account used to log on to the DEC portal and related online accounts.

3 Equipment

3.1 Damage or loss of equipment

3.1.1 Students are fully responsible for any damage or theft on the device they are using. Reimbursement may be required for school property. The Principal will, having regard to all the circumstances of the matter, determine whether the student is responsible for the damage to the device.

3.1.2 In circumstances where a device is damaged by abuse or malicious act of another student ("the other student"), the Principal will, having regard to all the circumstances of the matter, determine whether the other student is responsible for the damage to the device and whether costs incurred in the repair of the device should be borne by the other student.

3.1.3 The above clause does not bind students to the determination of the Principal.

3.1.4 Liability for damage or loss of peripheral equipment will in all circumstances be borne by the student.

4 Standards for equipment care

Students are responsible for:

(a) Taking due care of all device's in accordance with school guidelines.
(b) Adhering to the Department of Education's policy *Online Communication Services: Acceptable Usage for School Students* (PD/2002/0046/V04).
(c) Backing up all data securely. All electronic data and resources used for school coursework must be stored on another device or electronic medium accessible on demand. Students must not rely on the continued integrity of data on the school's device.

5 Misuse of equipment and communication systems

5.1 Standard school discipline procedures apply for misuse of the device contrary to this Student Acceptable Use of Technology Agreement or other school rules.

5.2 Examples of action the school may take in cases of misuse include:

(a) the student may not be able to use the device for the remainder of the lesson
(b) permission for the student to use any school device pursuant to the Student Acceptable Use of Technology policy may be revoked
(c) conventional discipline procedures including detention or suspension where deemed appropriate pursuant to the school's discipline procedures.

6 Acceptable equipment and communication system use

6.1 Use of the any device during the school day is at the discretion of teachers and staff. Students must use the device as directed by their teacher.

6.2 The primary purpose of the device at school is educational.

6.3 Students must NOT play any violent, offensive or inappropriate games or visit any such sites. Students witnessing anything falling under this category must report it to a teacher immediately.

6.4 Students are NOT to attempt to install programs or apps, make any changes to the settings or configuration on any school device. This includes but not limited to:

(a) Changing wallpaper settings etc
(b) Changing network settings etc
(c) Modifying folder properties or permissions
(d) Attempt to boot into a portable storage device
(e) Reinstall or modify the Operating System of the device

6.5 Students are NOT to create, participate in, or circulate content that attempts to undermine, hack into and/or bypass the hardware and software security mechanisms that are in place.

6.6 Students are NOT to unplug any cable or make any physical changes on any school device. This includes but not limited to:

(a) Power cables
(b) Network cables
(c) Peripheral devices, such as mouse's, keyboards etc
(d) adapters for the connection of video output or data transfer
(e) opening of device or removal of hardware

6.7 Students are NOT to connect any device or hardware to the school wireless or wired network. The only exception is your BYOD device to the wireless network. A BYOD agreement form must be signed by you and a guardian in this case.

6.8 Students are NOT to use software, apps or hardware to scan or discover the network. This includes:

(a) Intercepting traffic or data
(b) Gaining access or information on other devices than your own
(c) Modifying wireless and wired network configurations
(d) Attempting to disadvantage other students or staff on the network
(e) The creation of scripts/batch files to capture user credentials

6.9 Students are NOT to share confidential data relating to accounts and passwords. Your student portal and email account must NOT be shared or used by another student

6.10 Students will have access to the "Collaboration" network drive, this allows students and staff to upload files and collaborate with each other. Students are NOT to access, modify, move or delete another students or staff members file or folder. No offensive or inappropriate material is to be placed on this network drive. No clickbait or attempts to gain an advantage over a students or staff member's data or information will be tolerated.

6.11 Students are NOT to use the network for non-academic related bandwidth intensive activities such as network games, downloading/uploading large files or serving as a host for such activities.

6.12 Upon enrolment into a New South Wales Government school, parental/caregiver permission was sought to allow the student to access the Internet at school based on the Department of Education's policy *Online Communication Services: Acceptable Usage for School Students* (PD/2002/0046/V04). Extracts are provided below. This policy forms part of this Bring Your Own Device User Agreement.

6.13 The policy *Online Communication Services: Acceptable Usage for School Students* (PD/2002/0046/V04) applies to the use of the device and internet on the device:

(a) at school
(b) where in connection with a school-related activity, school-related program, including coursework, outside school.

Note: The complete *Online Communication Services: Acceptable Usage for School Students* (PD/2002/0046/V04) policy is available for viewing at:

https://education.nsw.gov.au/policy-library/policies/online-communication-services-acceptable-usage-for-school-students

Extracts: *Online Communication Services: Acceptable Usage for School Students*:

1. Objectives - Policy statement

1.1
The internet provides an opportunity to enhance students' learning experiences by providing access to vast amounts of information across the globe. Online communication links students to a collaborative learning environment and is intended to assist with learning outcomes. Today's students are exposed to online communication tools and the internet in their community. They have the right to expect secure access to these services as part of their learning experiences.

1.2
Use of the internet and online communication services provided by the department is intended for research and learning and communication between students and staff. Access to internet and online communication tools at school will assist students to develop the information and communication skills necessary to use the internet effectively and appropriately.

1.3
Responsible use of the services by students, with guidance from teaching staff, will provide a secure and safe learning environment.

1.4
Students using internet and online communication services have the responsibility to report inappropriate behaviour and material to their supervisors.

1.5
Students who use the internet and online communication services provided by the department must abide by the conditions of acceptable usage. They should be made aware of the acceptable usage policy each time they log on.

1.6
Students should be aware that a breach of this policy may result in disciplinary action in line with their school's discipline policy.

2. Audience and applicability

2.1
This policy applies to all school students located at NSW public schools who access internet and online communication services within the department network and from any external location.

3. Context

3.1
This policy document takes account of the Memorandum Student Access to the Internet of 18 July 1997 and the Memorandum DN/04/00215 – Review by Schools of their Student Access to the Internet Policies.

3.2
This policy document should be read as consistent with school discipline, child protection, anti-discrimination and anti-racism policies.

4. Responsibilities and delegations

4.1 Access and Security

4.1.1
Students will:
●not disable settings for virus protection, spam and filtering that have been applied as a departmental standard.
●ensure that communication through internet and online communication services is related to learning.
●keep passwords confidential, and change them when prompted, or when known by another user.
●use passwords that are not obvious or easily guessed.
●never allow others to use their personal e-learning account.
●log off at the end of each session to ensure that nobody else can use their e-learning account.
●promptly tell their supervising teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable.
●seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.
●never knowingly initiate or forward emails or other messages containing a message that was sent to them in confidence.
●a computer virus or attachment that is capable of damaging recipients' computers.
●chain letters and hoax emails.
●spam, e.g. unsolicited advertising material.
●never send or publish unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments.
●threatening, bullying or harassing another person or making excessive or unreasonable demands upon another person.
●sexually explicit or sexually suggestive material or correspondence.
●false or defamatory information about a person or organisation.
●ensure that personal use is kept to a minimum and internet and online communication services is generally used for genuine curriculum and educational activities. Use of unauthorised programs and intentionally downloading unauthorised software, graphics or music that is not associated with learning, is not permitted.
●never damage or disable computers, computer systems or networks of the department.
●ensure that services are not used for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.
●be aware that all use of internet and online communication services can be audited and traced to the e-learning accounts of specific users.

4.2 Privacy and Confidentiality

4.2.1
Students will:
●never publish or disclose the email address of a staff member or student without that person's explicit permission.
●not reveal personal information including names, addresses, photographs, credit card details and telephone numbers of themselves or others.
●ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests.

4.3 Intellectual Property and Copyright

4.3.1
Students will:
●never plagiarise information and will observe appropriate copyright clearance, including acknowledging the author or source of any information used.
●ensure that permission is gained before electronically publishing users' works or drawings. Always acknowledge the creator or author of any material published.
●ensure any material published on the internet or intranet has the approval of the principal or their delegate and has appropriate copyright clearance.

4.4 Misuse and Breaches of Acceptable Usage

4.4.1
Students will be aware that:
●they are held responsible for their actions while using internet and online communication services.
●they are held responsible for any breaches caused by them allowing any other person to use their e-learning account to access internet and online communication services.
●the misuse of internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

5. Monitoring, evaluation and reporting requirements

5.1
Students will report:
●any internet site accessed that is considered inappropriate.
●any suspected technical security breach involving users from other schools or from outside the NSW Department of Education.

5.2
Students should be aware that:
●their emails are archived and their web browsing is logged. The records are kept for two years.
●the email archive and web browsing logs are considered official documents.
●they need to be careful about putting their personal or sensitive information in emails or on websites.
●these records may be used in investigations, court proceedings or for other legal reasons.