Acceptable Usage of the Computer Network, Internet and Email Services

Policy Statement

Use of the Computer Network, Internet and Email services provided by Fort Street High School and the NSW Department of Education is intended for research and learning, and communication between students and staff. Access to Internet and email at school will assist students to develop the information and communication skills necessary to use the Internet effectively and appropriately.

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

Responsibilities and Delegations

Fort Street High School requires the responsible use of the Computer Network, Internet and Email for processing information to support school related work and research.

1. Access and Security

Students will:

- never damage or disable computers, computer systems or networks, or wilfully attempt to interfere with the operating programs and software of the school and DoE
- maintain the computer facilities as they have been set-up for use by the school community and must report any problems with hardware or software setup immediately to a supervisor
- not disable settings for virus protection, spam and filtering that have been applied as a departmental standard
- ensure that personal use is kept to a minimum and Internet and Email 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
- 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
- respect the privacy of other people's passwords and under no conditions reveal their password to other students
- ensure their own personal safety and that of others by not revealing the personal details of themselves or any other person on the internet
- use appropriate language
- report any sites containing offensive or inappropriate material
- report inappropriate behaviour and material to their supervising teacher
- 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 send/receive or publish:

  - unacceptable or unlawful material or remarks, including offensive, threatening, 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
  - material that is rude, obscene or dangerous.
- 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.
- 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 Email Services can be audited and traced to the e-learning accounts of specific users.

2. Privacy and Confidentiality

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.

3. Intellectual Property and Copyright

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
- 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
- observe all copyright laws with respect to software and the internet.

4. Misuse and Breaches of Acceptable Usage

Students must be aware that:

- they are held responsible for their actions while using the school's Computer Network, Internet and Email Services
- they are held responsible for any breaches caused by them allowing any other person to use their e-learning account to access the school's Computer Network, Internet and Email Services.

Students will report:

- any Internet site accessed that is considered inappropriate
- any suspected technical security breach involving users from other schools, TAFEs, or from outside the NSW Department of Education.

Consequences

- Students should be aware that breaches of this Policy may result in the withdrawal of access to the School Computer Network, Internet and Email
- Other actions may be required as specified in the Fort Street High School's Code of Conduct or Positive Expectation Policy.

Agreement to Acceptable Usage of the Computer Network, Internet and Email Services

To the Computer Coordinator and Principal

Student Agreement

I have read the *Acceptable Usage of the Computer Network, Internet and Email Services* for Fort Street High School as printed on the previous page. I understand fully and I agree to abide by the responsibilities as listed.

Student's Name: ______________________________________ Year: _______________

Student's Signature:____________________________________ Date: _______________

Parent Agreement

As the parent or guardian of the above student I have read the *Acceptable Usage of the Computer Network, Internet and Email Services* for Fort Street High School as printed on the previous page. I recognise that Fort Street cannot control the content of the internet and understand the School uses the controls that the DoE has provided.

I am aware of my child's agreement to the *Acceptable Usage of the Computer Network, Internet and Email Services* and that my child accepts responsibility for the appropriate use of the school's computer network, internet and email services.

I hereby give permission for my child to have access to the Fort Street High School computer network, internet and email services.

Parent or Carer's Name: ____

Parent or Carer's Signature: ____

Contact Number: __________________________ Date: ______________

Student Bring Your Own Device (BYOD) Guidelines

1. Introduction

Fort Street High School has adopted a *Bring Your Own Device* (BYOD) approach to allow student use of personal mobile electronic devices at school to access the NSW Department of Education Wi-Fi network.

The term “device” refers to any mobile electronic technology, including assistive technologies, brought into the school, which is owned by the student, and which has the capability of connecting to the department’s Wi-Fi network.

There are recommended devices listed on the school’s website http://www.fortstreet.nsw.edu.au/Student-Life/BYOD/. Mobile phones are not an appropriate device. Laptops or tablets that are capable of joining the school’s Wi-Fi network are appropriate.

2. Research

A literature review undertaken by the NSW Department of Education in 2013 found that the key considerations for implementing BYOD were:

- The widespread availability of wireless internet-enabled devices.
- The integral nature of these devices to the students’ own world.
- The possibility of leveraging students’ attachment to their own devices to deepen learning and to make learning more personalised and student-centred.

3. Access to the department’s Wi-Fi network and resources

3.1 Internet access through the department’s Wi-Fi network will be provided on departmental sites at no cost to students who are enrolled in NSW public schools.

3.2 Students will not have access to the local school network drives until hardware and software has been updated by the DoE.

4. Acceptable use of devices

The principal will retain the right to determine what is, and is not, appropriate use of devices at the school within the bounds of the department’s policies and NSW privacy and other legislation.

4.1 Students must comply with departmental and school policies concerning the use of devices at school while connected to the department’s Wi-Fi network.

4.2 Students must not attach any school-owned equipment to their mobile devices without the permission of the school principal or an appropriate staff member.

4.3 Students must not create, transmit, retransmit or participate in the circulation of content on their devices that attempts to undermine, hack or bypass any hardware and software security mechanisms that have been implemented by the department, its Information Technology Directorate or the school.

4.4 Students must not copy, transmit or retransmit any material that is protected by copyright, without prior permission from the copyright owner.

4.5 Students must not take photos or make video or audio recordings of any individual or group without the express written permission of each individual (including parent or carers consent for minors) being recorded and the permission of an appropriate staff member.

4.6 Students must not use the department's network services to seek out, access, store or send any material of an offensive, obscene, pornographic, threatening, abusive or defamatory nature is prohibited. Such use may result in disciplinary and/or legal action.

4.7 Students and their parents or carers must be advised that activity on the internet is recorded and that these records may be used in investigations, court proceedings or for other legal reasons.

Where the school has reasonable grounds to suspect that a device contains data which breaches the BYOD Student Agreement, the principal may confiscate the device for the purpose of confirming the existence of the material. Depending on the nature of the material involved, school disciplinary action may be appropriate or further action may be taken including referral to the police.

The consequences of any breaches of the school's BYOD policy will be determined by the principal in accordance with relevant Department policies and procedures and accepted school practice.

5. BYOD Student Agreement

5.1 Prior to connecting their devices to the department's Wi-Fi network, students must return a signed BYOD Student Agreement.

5.2 The BYOD Student Agreement must be signed by the student and by a parent or carer. If a student is living independently of their parents or carers or is 18 years of age or more, there is no requirement to obtain the signature of a parent or carer. Principals will make these determinations.

5.3 By accepting the terms of the BYOD Student Agreement, the student and parents or carers acknowledge that the student:

- agrees to comply with the conditions of the school's BYOD policy; and
- understands that noncompliance may result in disciplinary action.

Schools should retain a copy of the BYOD Student Agreement in print or electronic form and it should be kept on file with the student record.

6. Long-term care and support of devices

Students and their parents or carers are solely responsible for the care and maintenance of their devices.

6.1 Students must have a supported operating system and current antivirus software, if applicable, installed on their device and must continue to maintain the latest service packs, updates and antivirus definitions as outlined on the BYOD Student Responsibilities document.

6.2 Students are responsible for ensuring the operating system and all software on their device is legally and appropriately licensed.

6.3 Students are responsible for managing the battery life of their device. Students should ensure that their devices are fully charged before bringing them to school. Schools are not responsible for (or restricted from) providing facilities for students to charge their devices.

6.4 Students are responsible for securing and protecting their device in schools, and while travelling to and from school. This includes protective/carry cases and exercising common sense when storing the device. Schools are not required to provide designated or secure storage locations.

6.5 Students should clearly label their device for identification purposes. Labels should not be easily removable.

6.6 Students should understand the limitations of the manufacturer's warranty on their devices, both in duration and in coverage.

7. Damage and loss

7.1 Students bring their devices onto the school site at their own risk.

7.2 In cases of malicious damage or theft of another student’s device, existing school processes for damage to school or another student’s property apply.

8. Technical support

The school will provide initial support to enable students to join the DoE Wi-Fi network. There will be no other ongoing support provided to students as part of this initiative.

9. Insurance

Student devices are not covered by Treasury Managed Fund. Insurance is the responsibility of parents or carers and students.

10. DoE technology standards

The department’s Wi-Fi network installed in high schools operates on the **802.11n 5Ghz standard**. Devices that do not support this standard will not be able to connect.

11. Security and device management processes

Students will be responsible for:

- strong passwords (the portal has Password Help information);
- device anti-virus software, if applicable; and
- privacy controls.

The department’s Digital Citizenship (www.digitalcitizenship.nsw.edu.au) website contains information to support security and device management.

BYOD Student Responsibilities

Operating system and anti-virus:

Students must ensure they have a legal and licensed version of a supported operating system and of software. If applicable, students’ devices must be equipped with anti-virus software.

NSW Department of Education Wi-Fi network connection only:

Student devices are only permitted to connect to the department’s Wi-Fi network while at school. There is no cost for this service.

Battery life and charging:

Students must ensure they bring their device to school fully charged for the entire school day. *No charging equipment will be supplied by the school.*

Theft and damage:

Students are responsible for securing and protecting their devices at school. *Any loss or damage to a device is not the responsibility of the school or the Department.*

Confiscation:

Students' devices may be confiscated if the school has reasonable grounds to suspect that a device contains data which breaches the BYOD Student Agreement.

Maintenance and support:

Students are solely responsible for the maintenance and upkeep of their devices.

Ergonomics:

Students should ensure they are comfortable using their device during the school day particularly in relation to screen size, sturdy keyboard etc.

Data back-up:

Students are responsible for backing-up their own data and should ensure this is done regularly.

Insurance/warranty:

Students and their parent or carers are responsible for arranging their own insurance and should be aware of the warranty conditions for the device.

Bring Your Own Device (BYOD) Student Agreement

Students must read and sign the BYOD Student Agreement in the company of a parent/carer unless otherwise directed by the principal.

I agree that I will abide by the school's BYOD policy and that:

❒ I will use the department's Wi-Fi network for learning.

❒ I will use my device during school activities at the direction of the teacher.

❒ I will not attach any school-owned equipment to my mobile device without the permission of the school.

❒ I will use my own portal/internet log-in details and will never share them with others.

❒ I will stay safe by not giving my personal information to strangers.

❒ I will not hack or bypass any hardware and software security implemented by the department or my school.

❒ I will not use my own device to knowingly search for, link to, access or send anything that is:

- offensive
- pornographic
- threatening
- abusive or
- defamatory

- considered to be bullying

❒ I will report inappropriate behaviour and inappropriate material to my teacher.

❒ I understand that my activity on the internet is recorded and that these records may be used in investigations, court proceedings or for other legal reasons.

❒ I acknowledge that the school cannot be held responsible for any damage to, or theft of my device.

❒ I understand and have read the limitations of the manufacturer’s warranty on my device, both in duration and in coverage.

❒ I have read the BYOD Student Responsibilities document and agree to comply with the requirements.

❒ I have reviewed the BYOD Device Requirements document and have ensured my device meets the minimum outlined specifications.

❒ I have read and will abide by the NSW Department of Education *Online Communication Services – Acceptable Usage for School Students.*

Date: _____/______/_____

______________________________ in the presence of: __________________________

Student Name Parent or Carer’s Name

______________________________ __________________________

Student Signature Parent or Carer’s Signature