EPPING BOYS HIGH SCHOOL

213 Vimiera Road, EASTWOOD, NSW 2122
Ph: 9869 2701   Fax: 9868 1198   Email: eppingboy-h.school@det.nsw.edu.au
Principal: Timothy O'Brien, BEc, Dip Ed

Technology Acceptable Use Policy

This policy is an abridged version of the *Online Communication Services: Acceptable Usage for School Students* Policy developed by the NSW DEC to more accurately meet the needs of the Epping Boys High School community. The original document may be located at https://www.det.nsw.edu.au/policies/general_man/general/accep_use/PD20020046.shtml

This document defines the policy for school students of the NSW Department of Education and Communities for the appropriate and acceptable use of internet and online communication services provided by the Department.

The Melbourne Declaration on Educational Goals for Young Australians, (December 2008) highlights that access to, and appropriate use of, technology is essential for students to fully participate in their learning in the 21st century.

Rapid and continuing advances in information and communication technologies (ICT) are changing the ways people share, use, develop and process information and technology. In this digital age, young people need to be highly skilled in the use of ICT. While schools already employ these technologies in learning, there is a need to increase their effectiveness significantly over the next decade, (p.5. Melbourne Declaration on Educational Goals for Young Australians, December 2008).

This document forms the basis for technology use at Epping Boys High School. Using the principles outlined in this document, teachers will ensure that students understand how to use technology appropriately and effectively to maximize learning opportunities while being safe and being respectful of the law and others' rights.

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 provide 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 with the NSW Department of Education and Communities.

1.2 Use of the internet and online communication services provided by the NSW Department of Education and Communities 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 NSW Department of Education and Communities must abide by the Department's 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 NSW Department of Education and Communities network and from any external location.

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.

Students will 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 NSW Department of Education and Communities.

- 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, TAFEs, or from outside the NSW Department of Education and Communities.

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.