

STUDENT ELECTRONIC COMMUNICATION POLICY (7-12)

Internet, Intranet/LMS and Email

1. Purpose of the Policy

The purpose of this policy is to assist in preserving the integrity of the computer systems and information of the School and to provide guidelines for the use of the Electronic Communication Systems by students of St Paul's Anglican Grammar School. The Electronic Communication Systems includes, but is not limited to, all Internet and email activities and/or communications (and all related applications and Electronic Communication Systems).

This policy is to be read in conjunction with other statements and policies of the School, such as the Social Media, Mobile Electronic Devices, Bullying and Harassment and Student Use of Electronic Mobile Devices Policies and may be amended from time to time.

2. Policy Guidelines

The School provides access to the Electronic Communication Systems for the purpose of school-related work. The School may log, store and access the contents of emails and records of Internet browsing activities by all students and reserves all rights of access to this data. As such, students should not expect any communications on the Electronic Communication Systems to be private. Browsing of, and access to, the Electronic Communication Systems will be monitored from time to time by the School as deemed appropriate.

This policy has been introduced because the improper use of the School's Internet and e-mail system may:

- threaten the security or integrity of the School's information technology systems;
- affect the privacy and wellbeing of other students; and
- result in legal liability for the School and/or its employees.

3. Authorised Use

Student use of the School's electronic communication resources for legitimate school-related purposes is authorised with the issuing of an account. Students will be instructed in relation to passwords and access details. These passwords and access details must not be changed unless at the express direction of Information Technology Services.

Students are responsible for maintaining the security of their accounts and their passwords.

4. General Use

Students must only access the Electronic Communication Systems for purposes of individual research. Students must not access the Electronic Communication Systems for purposes unrelated to the School curriculum unless given express permission by School staff.

Students must not:

- interfere with the normal operation of the Electronic Communication Systems, including propagating computer viruses and sustained high volume network traffic which substantially hinders others in their use of the Electronic Communication Systems;
- examine, change or use another person's files, output, or user name without explicit authorisation;
- use another person's username and password without that person's consent;
- disclose passwords to persons other than authorised representatives of the School.

5. Internet and Intranet Use

Students are provided with access to the Internet and intranet for appropriate school-related purposes. In using the Internet and intranet, students must not:

- visit Internet or intranet sites, or transfer data from these to their hard drive or USBs, that contain, or receive, send or download any material that is offensive, obscene, pornographic, racist, sexist or defamatory, or which is intended to annoy, harass or intimidate another person;
- make or post on the Internet or intranet indecent remarks, proposals or materials;
- upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the School;
- subscribe to excessive or inappropriate List servers and Mail Groups.

6. Email Use

Email should be relevant and sent where it is considered to be the best form of communication. Students should limit their use of email during class to the sole purpose of communications directly related to the subject being studied in that class. During non-class time, students must limit their use of email to school-related activities.

Students may only use email to communicate about matters not related to the curriculum if they have the express permission of the appropriate Head of School.

Prior to sending any email, students should consider the likely format of the email when received (e.g. phrasing, type-facing etc.), the content of the email, and alternative and perhaps more effective forms of communication.

In composing emails students should:

- write well-structured emails and use short, descriptive subjects;
- use clear headings and appropriate salutations;
- use appropriate language and ensure that the content, form, grammar and spelling of all email messages meet the professional business standards required by the School prior to transmission;
- only send emails of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, using other means of communication, or protecting information by using a password; and
- only send attachments where necessary and appropriate.

Students must not:

- send unsolicited email messages, except for proper school-related purposes;
- send chain letters with or without attachments;
- forge or attempt to forge email messages;

- disguise or attempt to disguise identity when sending an email message;
- send email messages using another person's email account while claiming to be that person;
- copy a message or attachment belonging to another user without permission from the originator;
- write emails in capitals;
- encrypt emails without written permission from management; or
- use email as a filing system.

9. Privacy

Students expressly waive any right of privacy in anything they create, store, send or receive on the Electronic Communication Systems or any electronic device the student chooses to bring to School.

10. Prohibited Use of the Electronic Communication Systems

Prohibited uses of the Electronic Communication Systems include any conduct that:

- Violates or infringes the rights of any other person, including the right to privacy;
- Contains real or potentially defamatory, false, inaccurate, abusive, obscene, violent, pornographic, profane, sexually-explicit, sexually-oriented, threatening, racially-offensive or otherwise biased, discriminatory or illegal or any other inappropriate material;
- Has instructions on the manufacture and/or use of illegal and/or dangerous products, substances or materials or any other illegal or subversive activity;
- Breaches any other School policy, including prohibitions against harassment of any kind;
- Accesses intellectual property in a way that breaches intellectual property rights;
- Attempts or succeeds in obtaining unauthorised access to Electronic Communication Systems, attempts to breach any security measures on any such system, attempts to intercept any electronic transmissions without proper authorisation, or unauthorised use of a password/mailbox, including constructing electronic communication so that the communication appears to be from another person/organisation;
- Fails to use the system as prescribed, thus permitting infection by computer virus or deliberate infection by computer virus;
- Propagates chain emails or forwarding messages to groups or lists without the consent of the user;
- Results in unauthorised external access to the Electronic Communication Systems; or
- Offends or potentially offends the ethos, principles and/or foundations of the School.

The consequences of engaging in inappropriate use of the Electronic Communication Systems will vary according to the seriousness of the breach including but not limited to cancellation of enrolment.