St Paul's
ANGLICAN GRAMMAR SCHOOL

Electronic Communication Systems Policy (P-12)

Audience: School Community

1. Purpose of the Policy

The purpose of this policy is to assist in preserving the integrity of the School's computer systems and information and to provide guidelines for the use of these systems. Management Systems include, but are not limited to, all internet, chat and email activities and/or communications, MyStPauls, Microsoft 365 and Zoom, (and all related applications). For electronic communication systems not authorised by the School (eg. Tik Tok, Discord, etc…) please reference the policies below.

This policy is to be read in conjunction with other school policies, including:

- Electronic Device Guidelines (Junior)
- ICT Acceptable Use Agreement
- Mobile Phone and Other Electronic Devices Policy
- Bullying and Harassment Prevention Policy
- Online Learning and Video Conferencing Policy
- Internet Use and Social Media Policy

The additional purpose of this policy is to educate students of St Paul's Anglican Grammar School in the safe, appropriate and ethical use of information communication technologies.

2. Policy Guidelines

The School provides access to a range of Electronic Communication Systems for the purpose of school-related work. The School may log, store and access the contents from any of these systems, including emails, MyStPauls, Microsoft 365 (including Teams/Zoom) 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 and activity on the Electronic Communication Systems of the School to be private. Browsing of, and access to, the Electronic Communication Systems of the School will be monitored as deemed appropriate.

3. Protection

This policy has been introduced to protect the integrity of the School and its Electronic Communication Systems and to prevent misuse in the way of but not inclusive of the following:

- unauthorised access to the usernames/passwords and accounts of others
- threating the security or integrity of the School's information technology systems
- scams and spam emails
- unauthorised access to another user's laptop either physically or via remote administrative tools such as but not limited to PowerShell or Windows Command Prompt (CMD)
- distributed Denial of Service attacks (DDoS)
- phishing attacks
- malware, spyware and ransomware attacks
- Brute Force attacks
- social engineering/cyber fraud
- affect the privacy of students and employees of the School
- using technology to falsely represent or misrepresent others
- affect the wellbeing of other students, and employees of the School
- result in legal liability for the School and/or its employees

4. Authorised Use

Student use of the School's Electronic Communication Systems for legitimate school-related purposes is authorised with the issuing of an account for any of the School’s Electronic Communication Systems. Students will be instructed in relation to passwords and access details. These passwords and access details must be changed at least each semester and in according to the ICT Acceptable Use Agreement or the express direction of Information Technology Services.

All students are responsible for maintaining the security of their accounts and their passwords. Younger students in particular, will be assisted by their classroom teachers.

5. General Use

Students must only access the School’s Electronic Communication Systems for purposes of learning, seeking information relating to school activities and events e.g. SEISA training schedule and other school-related matters. Students must not access the Electronic Communication Systems for purposes unrelated to School curriculum or co-curricular activities, unless given express permission by School staff.

Students must not:

- interfere with the normal operation of the Electronic Communication Systems of the School, including propagatingcomputer viruses, unauthorized coding, and sustained high volume network traffic which substantially hinders others in their use of the School’s Electronic Communication Systems
- examine, change or use another person's files, output, or username 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

6. 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 belongingto parties outside of the School
- subscribe to excessive or inappropriate List servers and Mail Groups
- load games onto their school laptops or other school devices
- use their mobile phone or other personal devices to circumvent the filters or protocols for student internet or intranet use at the School

7. The use of e-mail, Social Stream and Teams Chat (Electronic Communication Systems)

Electronic communication should be relevant and sent where it is considered to be the best form of communication. Students should limit their use of electronic communication 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 electronic communication systems to school-related activities.

Students may only us Electronic Communication Systems 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 e-mail, students should consider the likely format of the electronic communication when received (e.g. phrasing, type-facing etc.), the content of the electronic communication, and alternative and perhaps more effective forms of communication.

In composing e-mails and all others forms of electronic communication students should:

- write well-structured e-mails and use short, descriptive subjects
- use clear headings and appropriate salutations (eg. Dear Mr Smith/Yours sincerely, Jane)
- use appropriate language and ensure that the content, form, grammar and spelling of all e-mail messages meet the professional business standards required by the School prior to transmission
- only send e-mails 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 e-mail, using other means of communication, or seeking help where needed
- only send attachments where necessary and appropriate

Students must not:

- send unsolicited e-mail messages, social stream or Teams chat, except for proper school-related purposes
- send chain letters with or without attachments
- forge or attempt to forge e-mail messages
- disguise or attempt to disguise identity when using electronic communication systems;
- send electronic communication using another person's e-mail account while claiming to be that person
- copy a message or attachment belonging to another user without permission from the originator
- write in capitals while using electronic communication unless grammatically relevant.
- encrypt e-mails without written permission from management
- use e-mail as a filing system

8. 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.

9. Prohibited Use of the School's Electronic Communication Systems

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

(a) Violates or infringes the rights of any other person, including the right to privacy

(b) 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

(c) Has instructions on the manufacture and/or use of illegal and/or dangerous products, substances or materials or any other illegal or subversive activity (eg. Terrorism)

(d) Breaches any other School policy, including prohibitions against harassment of any kind

(e) Records and/or distributes recording of others without their permission

(f) Accesses intellectual property in a way that breaches intellectual property rights

(g) 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

(h) Fails to use the system as prescribed, thus permitting infection by computer virus or deliberate infection by computer virus

(i) Propagates chain e-mails or forwarding messages to groups or lists without the consent of the user

(j) Results in unauthorised internal or external access to the Electronic Communication Systems (eg. Use of the Dark Web to attack the School's system or engage in other illicit/illegal activities)
(k) Sabotages the School ICT systems and their use in any way
(l) Engages in any illegal activities using information technology
(m) Offends or potentially offends the ethos, principles and/or foundations of the School

10. Use of the School's name

Students are expressly forbidden from creating social media groups of any kind, on authorized School or personal electronic platforms, that use the School's name or logo, without the express permission of the School.

The use of school images, including photographs of staff and other students (past or present) is also expressly forbidden without the permission of the School and/or the individuals themselves.

11. Consequences

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 and the involvement of police.

Policy History and Schedule

Version 1

Date Created: 21/10/2021
Approved By: Operations
Date Approved: 26/10/2021
Author: MEB
Reviewed: 24/04/2023
Date of Next Review: 24/04/2025