

Acceptable Use of ICT for Students' Policy

Policy Owner	The Governing Body of The Sycamore School		
Version	1.2	Supersedes	1.1
Status	Draft	Updated By	Sonya Amor
Approved By	The Governing Body of The Sycamore School	Date of Approval	21 May 2020
Review Period	Every 2 years	Scheduled Review Date	May 2022

Purpose	To manage the appropriate use of information, communication and technology services by students at school, including the appropriate use of personal electronic devices (PEDs) by students at school.
---------	---

Scope	Students including full-time or part-time.
-------	--

References	Cybersafety in Qld State Schools – Qld Government and Safe Use of Digital Technologies www.esafety.gov.au
------------	--

Associate Policies and Supporting Documents	This should be read in conjunction with: <ul style="list-style-type: none"> • Code of Conduct/Behaviour Policy • Performance and Misconduct Policy • Social Media Policy • Anti-Bullying Policy • Anti-Harassment Policy • Anti-Discrimination Policy • Privacy Policy
---	---

Policy Statement:	<p>All students at The Sycamore School may be required to utilise ICT services for the purposes of learning. The Sycamore School expects this technology to be utilised to its full capacity to provide the most valuable learning for the benefit of all. The Sycamore School also expects students to demonstrate acceptable use via safe, lawful and ethical behaviour whenever using ICT services.</p> <p>This Policy applies to the management of all types of ICT services, as defined in the "Definitions" section below. This Policy also applies on the school premises, as well as during school activities, such as excursions, camps and extra-curricular activities whenever The Sycamore School ICT services are utilised. It also applies to all Sycamore owned equipment and services (e.g, internet activity) at all times irrespective of physical location.</p> <p>The Sycamore School reserves the right to restrict student access to ICT services if access and usage requirements are not met or are breached. Students should also note that breaches of this Policy may result in disciplinary action or criminal proceedings.</p>
-------------------	---

Definitions:	Personal Electronic Device (PED) – includes all types of mobile and smart phones, laptops, tablets, cameras and video recorders, hand-held game devices, music devices, USBs, PDAs, eBook readers, other palm and handheld devices and other equipment, as determined by the school, and owned by students.
---------------------	--

Responsibilities:	<p>School Responsibilities</p> <ul style="list-style-type: none"> • The Sycamore School acknowledges its responsibility to develop and implement this Policy to ensure the full utilisation of ICT services as an essential learning tool within acceptable use parameters. • Communicate this Policy to students and parents, ensuring that it is understood and acknowledged by students and parents annually See Appendix A. • Implement risk management measures to reduce the likelihood of network access to harmful information: <ul style="list-style-type: none"> ○ including monitoring/auditing internet and email activities, ○ keeping appropriate records, and ○ monitoring and reporting on any issues related to inappropriate ICT services. <ul style="list-style-type: none"> ▪ Any accidental access to inappropriate internet sites or where access to a site leads to inappropriate content students must report this to the ICT Manager immediately • Encourage students and parents to contribute to a healthy school culture. <p>Student Responsibilities</p> <p>Examples of acceptable activities in the use of ICT for students include, but are not limited to:</p> <ul style="list-style-type: none"> • Undertaking assigned class work and assessments • Authoring text, artwork, audio and visual material • Conducting research • Communicating or collaborating with other students, teachers, parents or experts • Accessing online references such as dictionaries, encyclopaedias and so on • Research and learning through the School's e-learning environment • Developing appropriate literacy, numeracy, communication and information skills. <p>ICT Security</p> <ul style="list-style-type: none"> • Use of the School's ICT network is secured with a username and password. The password must be strong enough so as not to be guessed by other users and is to be kept private by the student and not divulged to other individuals • Students cannot use another student or staff member's username or password to access the School network, including not trespassing in another person's files, home drive, email or accessing unauthorised network drives or systems • If a student suspects their username/password is being used by another person, it is their responsibility to inform their class teacher/ICT Manager and arrange for their password to be changed immediately. Failure to do so will mean the student will be held liable for what happens within their account • Students should not divulge personal information (e.g. name, parent's name, address, phone numbers), via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school • Students need to understand that copying of software, information, graphics or other data files may violate copyright laws without warning and be subject to prosecution from agencies that enforce such copyrights.
--------------------------	--

Responsibilities for using a PED

- No personal devices such as mobile phones and iPads are permitted in classrooms. They must be handed in at Reception each morning and collected at the end of the school day
- Students are responsible for the security, integrity, insurance and maintenance of their own personal devices and their network accounts
- Any inappropriate material or unlicensed software must be removed from PEDs before bringing the devices to school and such material is not to be shared with other students
- If students are found to have a personal device with them in the classroom it will be confiscated by school staff with its collection to occur at the end of the school day where the device is not required for further investigation.

Behaviour

It is unacceptable for students while at school to:

- Use the ICT facilities and devices (including PEDs) in an unlawful manner
- Download, distribute or publish offensive messages or pictures
- Install, copy, share, or download unauthorised software/applications
- Use obscene, inflammatory, racist, discriminatory or derogatory language
- Use language and/or threats of violence that may amount to bullying and/or harassment, or even stalking (including cyberbullying)
- Insult, harass or attack others or use obscene or abusive language
- Damage computers, printers or network equipment
- Commit plagiarism or violate copyright laws
- Ignore staff directions for the use of social media, online email and internet chat
- Send chain letters or spam email (junk mail)
- Knowingly download viruses or any other programs capable of breaching the network security
- Use in-device cameras anywhere a normal camera would be considered inappropriate
- Invade someone's privacy by filming/recording personal conversations or daily activities and/or the further distribution (e.g. forwarding, texting, uploading, Bluetooth use etc.) of such material
- Undertake hacking or intention to breach School security, copyright breaches, pirating and loading of unauthorized discs, and other storage devices onto the School system. This is a breach of this policy and will result in action being taken.
- Sites for personal use such as personal web spaces, chats/forums and other personal sites are not to be accessed at School
- Students must be aware electronic communication is not guaranteed to be private and all email should be considered a public document. System administrators of the network have access to all mail sent and received and automatic filtering of e-mails and internet use occurs
- Students will not agree to meet with someone they have met online without their parent/carer's approval
- Filtering of websites does occur but any accidental access to inappropriate internet sites must be reported immediately or if students receive inappropriate emails from anyone.

	<p>The School reserves the right to:</p> <ul style="list-style-type: none"> • Monitor and record all usage of its computer networks, including internet services by regularly filtering the network for inappropriate/non-education files and if found, delete these automatically. This includes staff emails. • Restrict access to internet and intranet services, where necessary • Cull/archive student files to remove unnecessary files and/or to regain disc space • Take disciplinary action when breaches of expected behaviour occur. <p>The School monitors and reports on intranet, internet and network usage and inspects email messages sent or received by anyone using the School’s ICT facilities and devices to:</p> <ul style="list-style-type: none"> • Identify inappropriate use • Protect system security • Maintain system performance • Protect the rights and property of the School. <p>Parent Responsibilities</p> <p>At The Sycamore School parents/carers have a responsibility to:</p> <ul style="list-style-type: none"> • Read and understand, and ensure their child reads and understands, this Policy to enable appropriate access and usage requirements, including the acceptable and unacceptable behaviour requirements • Encourage appropriate internet use by their children outside the school environment when using a PED • Encourage their children to behave in line with ICT safe practices. The School will educate students regarding cyber bullying, safe internet and email practices, and health and safety regarding the physical use of ICT devices.
<p>Implementation</p>	<ul style="list-style-type: none"> • Awareness – regularly raise awareness of acceptable ICT usage and obtain agreement to abide by the requirements set out in Appendix A at the beginning of each year. • Training – regularly educate students • Culture - encourage students to contribute to a healthy school culture.
<p>Appendices</p>	<ul style="list-style-type: none"> • Appendix A – Student Code of Conduct for ICT Use Declaration

If more space is required, please attach an extra page.	

Please use the link below to help guide this process.

<https://www.classification.gov.au/classification-ratings/latest-classification-decisions>

Please complete and sign document, then return to the school.

_____ in the presence of: _____
 Young Person's Name Parent/Caregiver Name

_____ Parent/Caregiver Signature
 Young Person's Signature

_____ Date
 Date

OFFICE USE ONLY

Form completed, signed by both parties and returned. Date _____
 Internet Connection Approved Yes/No