Policy 9.4

ACCEPTABLE USE OF ICT (STUDENTS)

INTRODUCTION

Walford is a safe and supportive school. This policy describes the expectations for student use of information and communication technologies (ICTs) at Walford Anglican School for Girls. Walford is committed to ensuring that the use of ICTs and social media does not place students at risk, and that the wellbeing and safety of students is protected.

These guidelines are led by the Wellbeing Team and are shaped by our School values.

DEFINITIONS

A safe and supportive school – is a school where the risk from all types of harm is minimised, diversity is valued and all members of the school community feel respected and included.

Staff – those people employed by the school to undertake various roles and responsibilities, including teaching and administration.

Parent – parents, legal guardians and caregivers.

ICTs – information and communication technologies. ICT is defined, for the purpose of these guidelines, as:

- School wide and local area networks (both wired and wireless) including wiring, hubs, routers, transmitters/receivers and other devices;
- On premise and cloud servers and application software packages or services;
- Devices (desktop and laptop computers, mobile phones and tablets) and equipment (printers/copiers, projectors, speakers, headsets and other peripherals);
- Digital resources, learning resource management systems and distance learning systems; and
- Telephone systems including primary systems, conferencing and integrated voice response management systems and automatic dialling systems and video capturing, broadcast, receiving and distribution systems.

Cyber safety – the safe use of the Internet and ICT equipment/devices, including mobile phones.

Cyber bullying – bullying which uses digital technology as a means of victimising others. This includes the use of technology to harass others either directly or in-directly with the intention of causing harm. Such technology includes but is not limited to – email, SMS, Social Media or Discussion groups.

Examples include communications that seeks to intimidate, control, manipulate, put down or humiliate the recipient.

Digital footprints - are traces left behind by someone's activity in a digital environment. These traces can be analysed by the school or the police.

Sexting – is where a person takes a sexually-explicit digital photograph of him or herself or of someone else, and distributes it via MMS, Social Media or other messaging services. These images can then be posted on the internet or forwarded electronically to other people. Once posted on the internet these images can leave a permanent digital footprint and be accessed at any time in the future. It is illegal to take sexual photos or videos of children and young people.

Social media – sites that offer people new and varied ways to communicate via the Internet. These sites are often uncensored and both parents and children need to be aware of the risks in using these services.

School ICT – refers to the school's network, internet access, computers, licenced software, data, and other Technology and equipment controlled by the school, weather it is on or off campus.

ICT equipment/devices – includes but is not limited to digital devices (such as desktops, laptops, phones and tablets), storage devices (such as USB and SD Cards), cameras (such as video and digital cameras and webcams), all types of mobile phones, gaming consoles, video and audio players/receivers, 3D Printers, VR Goggles, laser cutters and any other similar technologies.

Inappropriate material – means material that deals with matters such as sex, cruelty or violence in a manner that is likely to be injurious to children or incompatible with a school environment.

Cyber Crime – occurs when computers or other electronic communication equipment/devices (e.g. Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.

Malware – 'malicious software' means software programs designed to cause damage and other unwanted actions on a computer system. Common examples include computer viruses, worms, spyware and trojans.

Personal use – means all non-work related use, and includes internet usage and private emails.

Artificial Intelligence (AI) – refers to computer systems or software that perform tasks normally requiring human intelligence, such as understanding language, recognising patterns, generating text or images, making predictions, or providing recommendations.

Wearable devices – are electronic technologies or smart accessories designed to be worn on the body that can collect, transmit, or display data. Examples include smartwatches, fitness trackers, and augmented reality glasses.

GUIDING PRINCIPLES

Walford is committed to ensuring that online behaviour demonstrates respect for the dignity of other people, and compliance with the laws in terms of copyright, privacy and confidentiality. In alignment with the Australian Student Wellbeing Framework, Walford is committed to building a respectful and positive learning environment that is safe, inclusive and supportive for all students.

Staff work collaboratively to develop a safe and respectful school community through a whole-school approach. Accepting responsibility for developing and sustaining safe and supportive learning and teaching communities that also fulfil Walford's child protection responsibilities.

An inclusive and connected school culture
Underpinned by our School value of Community, we encourage the active participation of all School community members in developing and maintaining a safe school community where diversity is valued.

Authentic student participation
Students actively participate in their learning and wellbeing outcomes. Students use their social and emotional skills to be respectful, resilient and safe.

Effective family and community partnerships
Staff work with families and communities to support both student learning and wellbeing. Being safe and supported at school is essential for student wellbeing and effective learning.

Providing support for wellbeing and positive behaviour.
Bespoke wellbeing programs teach students social emotional skills and develop their understanding to keep themselves and others safe and included.

If staff become aware of an issue relating to child protection and if they suspect child abuse and neglect they are required to make a mandatory notification to the Child Abuse Report Line (13 14 78).

ARTIFICAL INTELLIGENCE
Walford is guided by the Australian Framework for Generative Artificial Intelligence (AI) in Schools.

Teaching and learning
Generative AI tools are used to support and enhance teaching and learning

Human and social wellbeing
Generative AI tools are used to benefit all members of the school community.

Transparency
School communities understand how generative AI tools work, how they can be used, and when and how these tools are impacting them.

Fairness
Generative AI tools are used in ways that are accessible, fair, and respectful.

Accountability
Generative AI tools are used in ways that are open to challenge and retain human agency and accountability for decisions.

Privacy, security and safety
Students and others using generative AI tools have their privacy and data protected.

ACCEPTABLE AND UNACCEPTABLE USE OF ICTs

Acceptable use of ICTs may include:

- Use of the school's network in connection with curricular, co-curricular or pastoral activities.
- Sending and receiving emails using an appropriate school email account.
- Using the internet in connection with teaching and learning and along guidelines established by teaching staff.
- Accessing Cloud services as part of the school digital curriculum.
- Use teacher-approved AI tools to assist with research, revision, idea generation, or understanding difficult concepts.

Unacceptable actions or intent may include (but are not limited to):

- Excessive personal use, or personal use that breaches the Acceptable Use of ICTs Policy.
- Bullying, invading privacy, defaming or harassing individuals through messaging, emails, posting of blogs, wikis and/or images on web-based sites.
- Copyright infringement.
- Illegal or unlawful activity, including but not limited to:
    - Breach of copyright laws, licence agreements or any other legislation;
    - Blackmail and threats;
    - Accessing or distributing offensive, inappropriate or defamatory material;
    - Accessing or distributing material which could constitute racial or religious vilification, or unlawfully discriminatory material;
    - Accessing or distributing child exploitation materials;
    - Stalking; and
    - Mass distribution of malware and/or spam.
- Hacking accounts of other users, accessing passwords or transgressing school protective measures).
- Damaging or modifying the computer network (e.g. by introducing viruses, hacking, changing software settings, installing software, or damaging hardware).
- Using another person's password, disclosing a password to someone or impersonating someone.
- Interfering with another person's computer.
- Trespassing in another person's storage folder or storing files in unauthorised folders.
- Using the network for commercial or profit-making exercises.
- Deliberate misrepresentation of the School or its actions.
- Downloading information from the School network in order to provide it to an unauthorised third party.
- Disabling, interfering with or overloading any computer system or protective measure.
- Downloading or transferring illegal file types or subscribing to inappropriate email lists.
- Downloading or transferring games.
- Bringing inappropriate files, including games from home, via storage devices or e-mail (including USB memory sticks, and other storage devices).
- Disclosing personal details such as home address or phone number in a public forum such as a public chat or bulletin board.
- Using the School network to contravene any school rules.
- Recording staff, teachers or other students, intentionally or otherwise, without their express permission.
- Submitting AI-generated work as their own, or use AI to complete assessments or assignments dishonestly.
- Inputting identifying, private, or confidential information (about themselves, other students, or the School) into AI tools.

- Employing AI to monitor, record, imitate, or alter images, voices, or text of others without consent.

Electronic communication and work created via the School's network is not private, and the School may access their storage files to check for compliance with this policy.

INTERNET USE

The internet provides an opportunity to enhance students' learning experiences by providing access to vast amounts of information across the globe.

Use of the internet is intended for research and learning and communication between students and staff.

Access to internet tools 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.

Students using the internet have the responsibility to report inappropriate behaviour and material to their teachers.

Walford is committed to ensuring that internet use and access is appropriate.

EMAIL USE

When using email communication students should be aware that:

- While reasonable care is taken, a school cannot guarantee the confidentiality of online communication by users of the School's network.
- The email system is monitored by the School, emails are traceable and may also be recovered.
- Emails may be sent to the wrong destination and cannot always be recalled.
- If used carelessly, emails or attachments to emails can cause offence and in extreme cases may give rise to litigation.
- The tone of a written communication may be subject to an interpretation different from the one intended.
- Any email sent from the School's network is the property of the School and will necessarily reflect on the School.
- Email correspondence is no different from paper documents and can be requested by parents or other parties.
- Defamatory, sexually explicit, harassing, insulting or offensive material must not be sent to others, and students must not solicit such materials to be sent.

When using email communications, students should.

- Use the same guidelines, e.g. salutations as would be used with other types of correspondence, and observe the same conventions as with any other correspondence. Individuals should use appropriate language and check emails for typographical and spelling errors before sending.
- Use great caution in the language and tone used in an email.
- Never send an email in haste or anger.
- Delete all addresses of other recipients when forwarding a message.

- Place multiple addresses in the Blind Carbon Copy ("BCC") line if you wish to avoid recipients reading each other's email addresses.
- Scroll through an email before forwarding to make sure that you are only forwarding the intended message.
- Obtain the author's permission when forwarding personal or sensitive emails.
- Be aware that it may not always be appropriate to open or reply to an email from an unknown source. Attachments and emails from unknown origins should be deleted without opening them to view the contents.
- Limit the contents of an email to one subject, thus minimising the possibility of inadvertently forwarding inappropriate messages.

DIGITAL DEVICES

The rules for student personal digital devices are as follows.

Phones and personal communication devices

- Students in the Junior School should not bring phones to school.
- Students in Middle School are strongly discouraged from bringing personal digital devices to school.
- Student phones should be locked in lockers between 8.30am and 3.30pm for Secondary School students. Phones may only be accessed before school, after school, or with the explicit permission of a member of staff.
- Student phones should not be used or visible upon entry to School property or used or visible on campus in locker rooms or any other space.
- Student phones should not be mirrored to learning devices.
- Phones are not to be used for messaging, photography, recording or internet access during the school day, unless with the explicit permission of a member of staff.

Wearable devices

Students are not permitted to wear or use any wearable device that has the capability to record, photograph, message, or access the internet during the school day or at school events, unless explicitly authorised for educational or medical purposes.
Permitted devices (e.g., simple fitness trackers) must have communication and recording functions disabled. Any use of wearable technology must uphold the School's values of respect, privacy, and integrity.

- Student smart watches are only permitted at School if 'school mode' or 'airplane mode' is enabled; all notifications, recording capabilities and internet access capabilities should be disabled during school hours.

With the exception of smart watches (on 'airplane mode') and fitness trackers without communication or recording features, no wearable digital devices (e.g. wearable cameras, smart glasses, smart jewellery, smart earbuds, smart clothing) are permitted at School.

Learning devices

- Student learning devices should have notifications disabled during school hours and while on School property, including for co-curricular activities.
- Headphones, including airpods, may only be worn at School or on School property at the direction of the teacher.
- All other digital devices may only be used at the direction of School staff.

SOCIAL MEDIA

Social networking sites, blogs (web logs) and personal web sites are documents that are published within the public domain.

The public nature of these documents means that anyone can read them, including the school itself, a prospective employer or a person seeking information about someone's personality, political or religious views.

When using social media, students must ensure that they:

- Adhere to all State and National laws.
- Utilise cyber-safety strategies and instructions when using social media, including using restrictive privacy settings;
- Are aware that actions outside of school hours that impact the wellbeing of others and the school environment can result in possible suspension or other ramifications.
- Avoid involvement or accessing content or activities that could put safety at risk, or the privacy, safety or the school, other students, or members of the School community;
- Do not post material that is offensive, obscene, defamatory, bullying, abusive, harassing, threatening, discriminatory, hateful, racist, sexist, a breach of a court suppression order, or is otherwise unlawful;
- Do not harm the reputation and good standing of the school or those within its community;
- Do not seek friendships with teachers via social networking pages or join a teacher's page (except if the student is an immediate relative of the staff member; there should be no initiating of social media interaction by an old scholar within six months of a student completing Year 12, regardless of where schooling was completed); and
- Do not impersonate or falsely represent another person.

Students should be aware that no matter what protections they place around access to their personal sites, their digital postings are still at risk of reaching an unintended audience and being used in unintended ways.

NON-COMPLIANCE OR BREACH OF POLICY

Students must sign an Acceptable Use of ICT for Students Agreement, and adherence to the policy is a condition of student enrolment.

Non-compliance with the policy will be regarded as a serious matter and appropriate action will be taken. Depending on the nature of the inappropriate use of ICTs, non-compliance with Walford's Acceptable Use of ICTs Policy may constitute:

- A breach of school enrolment obligations;
- A breach of the Student Code of Behaviour or other School policy;
- An infringement of the privacy of other persons;
- A threat to the security of the School;
- Exposure to legal liability;
- Bullying, harassment, or sexual harassment;
- Unlawful discrimination; and/or
- A criminal offence.

Where there is a reasonable belief that illegal activity may have occurred, this will be reported to the South Australian Police (SAPOL).

LEGISLATIVE CONTEXT

Education and Early Childhood Services (Registration and Standards) Act 2011 (SA)
Children and Young People (Safety) Act 2017 (SA)
Copyright Act 1968 (Cth)
Equal Opportunity Act 1984 (SA)
Privacy Act 1988 (Cth)
Sex Discrimination Act 1984 (Cth)

RELEVANT STANDARDS AND FRAMEWORKS

Australian Student Wellbeing Framework
Child Protection Curriculum – Information for Educators
Protective Practices for Staff in Their Interactions with Children and Young People (SA)

Australian Framework for Generative Artificial Intelligence (AI) in Schools

Date Issued:	January 2021
Last Reviewed:	October 2025
Next Review:	October 2026
Responsibility:	Principal
Policy Number:	9.4