Acceptable Use of Information and Communication Technology Policy

Purpose	The purpose of this policy is to establish clear expectations and guidelines for the responsible, ethical, and secure use of all ICT resources within The River School, including school-owned ICT resources as well as personal ICT devices when they are used for school-related activities.	
Scope	This policy applies to students, parents and employees of The River School, including full-time, part-time, permanent, fixed term and casual employees, as well as contractors, volunteers and people undertaking work experience or vocational placements while they are in class, on school grounds or involved in school activities on or off school grounds.	
Responsibility	School Principal	
References	• *Privacy Act 1988 (Cth)* • *Copyright Act 1968 (Cth)* • Australian Privacy Principles • The Australian Student Wellbeing Framework • National Principles for Child Safe Organisations • eSafety Toolkit for Schools Student Behaviour Management Policy Bullying Prevention Policy Child Protection Policy Code of Conduct Privacy Policy Complaints Handling Policy Privacy Act 1988 (Cth) Copyright Act 1968 (Cth) Australian Privacy Principles The Australian Wellbeing Framework National Principles for Child Safe Organisations eSafety Toolkit for schools	
Status	Approved	**Supersedes** Acceptable Use of Personal and School electronic Devices Policy 2020
Authorised by	School Board	
Last Review Date	October 2026	**Next Review Date** October 2028
Review Cycle	Every 2 years	**Version ID** AUPSED 2026
Authorisation	Board Chair	**Date of Authorisation** April 2026
Policy Owner	AME Ltd Board	

Definitions

- Acceptable use: Use of technology that aligns with the values and purposes of the school and the intent of this policy, complies with relevant laws and regulations, and respects the rights of others.
- AI tools: Computer programs that utilise machine learning algorithms and other advanced techniques to mimic human cognitive abilities like reasoning, pattern recognition, and learning from data. These tools can generate creative content, assist with problem-solving, and automate certain tasks.
- Copyright: Legal protection granted to original creative works.
- Cyberbullying: Repeated online harassment or intimidation targeting an individual.
- Data: Any information stored or transmitted electronically, including personal or sensitive information of students and staff.
- ICT: Information and Communication Technology. Refers to all technology provided by the school used for collecting, storing, processing, transmitting, and communicating information, including computers, networks, software, applications, and internet access, and personal devices used for school-related activities.
- Network resources: Hardware and software infrastructure supporting the school's technology network.
- Personal device: Any electronic device owned by a user that is brought to school or used for school-related activities, such as laptops, phones, tablets, smart watches, etc.
- Plagiarism: Using someone else's work or ideas without conferring appropriate credit.
- School-related activities: Any activity connected to the school, including classes, breaks, assignments, clubs, extracurricular activities, school trips, and online communication of teachers and students.
- User: Any individual authorised to use school ICT, including staff, students, volunteers, authorised guests, and contractors.

1. Policy Statement

All students and employees have at The River School have the right and responsibility to utilise ICT services as essential teaching, learning and business tools. The River School expects this technology to be utilised to its full capacity to provide the most valuable learning and teaching environment to the benefit of all. The River School expects students and employees to demonstrate acceptable use via safe, lawful and ethical behavior whenever using ICT services. This Policy applies to the management of all types of electronic devices/ gadgets, including but not limited to: mobile and smart phones, smart watches, computers, laptops, tablets, iPods, iPads, cameras, video recorders, hand-held game devices, music devices, USBs, PDAs (personal digital assistant) and eBook readers.
This Policy applies on the school premises, school buses and related school activities, such as excursions, camps and extra-curricular activities.

2. Acceptable Use of ICT

General Principles

- All ICT use must be responsible, ethical, and legal, respecting the rights and dignity of others.

- ICT should be used to support learning, communication, and collaboration within the school community.
- ICT should be used in a way that maintains a safe and productive learning environment for all.
- To ensure the responsible and safe use of the school's network, The River School reserves the right to monitor and maintain appropriate records of network activity (e.g. email, web browsing, file sharing). This monitoring is conducted in alignment with applicable laws to protect the school community and maintain a secure learning environment.

Online Conduct

- Using ICT to engage in any illegal activity, such as hacking, accessing or distributing illegal content, or participating in online scams is strictly prohibited.
- Users must not engage in any online behaviour that is intended to intimidate, humiliate, threaten or harass another person, including sending offensive messages, excluding others from online groups with the intent to ostracise, spreading false or harmful information, or impersonating others.
- Sharing content online that is hateful, discriminatory, promotes violence or illegal activities, or expresses discriminatory views based on protected characteristics such as race, religion, gender, sexual orientation, disability, or any other personal attribute is strictly prohibited.
- Users must not engage in activities that violate community standards of decency and professionalism regarding online content. This includes accessing, viewing, or distributing materials of a sexually suggestive or exploitative nature.

2.1. Mobile phones

The policy of The River School is to allow the use of mobile and smart phones in limited circumstances as outlined below, while emphasising that in most circumstances students and staff will not need phones as they can access school phones and school personnel if they need to communicate outside of the school.

Users are responsible for the security and appropriate use of their personal devices on school premises. The school assumes no responsibility for their loss, theft, or damage.

Acceptable Use of Mobile Phones – Student specific

2.1.1. The use of personal phones during school hours is not allowed unless permission has been sought and given by the Principal. Refer to clause 2.1.4.

2.1.2. Personal phones are to be handed into the office on arrival at school and collected at the end of the school day.

2.1.3. Students should be aware that personal phones not handed into the office are likely to be confiscated for the rest of the day and parents notified. Parents are reminded that in the case of emergency the school office remains a vital and appropriate point of contact.

2.1.4. While on school related activities, outside school hours or off school grounds, where permission has been given to carry personal mobile/smart phones, students are to restrict use to agreed rules determined by the type of activity in consultation with the staff member responsible for the activity.

2.1.5. It should be noted that it is a criminal offence to use mobile/smart phones and other devices to menace, harass or offend another person - see *Online Conduct.* Students who use their phones to engage in personal attacks, harass another person, or post private information about another person using SMS messages, taking or sending photos or objectionable images or

bullying other students, or who use vulgar, derogatory or obscene language while using a mobile phone will have their phones confiscated for a period decided by the Principal, and their right to bring a phone to school will be revoked. Students should note that, in extreme cases, the school may consider it appropriate to involve the police.

2.2. Acceptable Use of mobile phones – Staff specific

Staff personal use of mobile phones will be confined to break times, when not on duty, and after school (except in the case of an emergency).

2.3 Acceptable Use of Other Electronic Devices

There are a number of other electronic devices including laptops, tablets, cameras and video recorders, hand-held game devices, music devices, USBs, PDAs, eBook readers, iPods, iPads, smart watches etc. that may be bought to School in certain circumstances while adhering to the Acceptable Use in this policy and outlined below.

Users are responsible for the security and appropriate use of their personal devices on school premises. The school assumes no responsibility for their loss, theft, or damage.

Acceptable Use of other electronic devices – Student specific

2.3.1. All personal electronic devices must be signed in at the office on arrival at school and their purpose for use at school stated. If permission has been granted for use during a school activity, the electronic device can only be used for the agreed purpose. At all other times, electronic devices must be kept at the office.

2.3.2. Personal, electronic devices without permission for use in a school activity are to be handed into the office on arrival at school and collected at the end of the school day.

2.3.3. Students should be aware that any personal, electronic devices not handed into the office are likely to be confiscated for the rest of the day and parents notified.

2.3.4. While on school related activities, school buses, outside school hours, or off school grounds, where permission has been given to use personal, electronic devices, students should restrict use to agreed rules determined by the type of activity in consultation with the staff member responsible for the activity.

2.3.5. It should be noted that it is a criminal offence to use any electronic device to menace, harass or offend another person - see *Online Conduct.* Students who use their or another person's device to engage in personal attacks, harass another person, or post private information about another person, taking or sending photos or objectionable images or bullying other students, or who use vulgar, derogatory or obscene language while using an electronic device will have the device confiscated for a period decided by the Principal, and their right to have their device at school will be revoked. Students should note that, in extreme cases, the school may consider it appropriate to involve the police.

2.3.6 Recording audio or video with personal devices during school-related activities without the express consent of all individuals involved and in contravention to relevant laws and school policies is strictly prohibited.

3. Access and Authorisation

- Access to school technology is granted on a privilege basis and for approved school-related purposes only.

- Limited personal use of school technology may be permitted for staff members during off-duty hours and within the acceptable use parameters outlined in this policy, as long as it doesn't interfere with official duties and incur more than negligible costs.
- Downloading and installing unauthorised software using school technology, including games, gambling software, pirated software, or applications that bypass school security measures or disrupt network performance, is strictly prohibited.
- Users must only access school technology using their own authorised accounts. Sharing of authorised accounts or passwords is strictly prohibited.
- Accessing data or systems that users are not authorised to access, or attempting to bypass security measures to gain unauthorised access is strictly prohibited.
- Users must not share confidential information with unauthorised individuals or organisations.

4. Data Security and Privacy

- Users should be aware of the risks of online activity and take steps to protect their own data and privacy.
- Users must not collect, store, or share personal information about others without their consent.
- All personal information, including sensitive information, must be handled confidentially and with appropriate security measures to protect against unauthorised access, misuse, or disclosure.
- Users must report potential data breaches or security vulnerabilities in alignment with the The River School Privacy Policy and Data Breach Response Plan.
- Users should limit use of AI tools at The River School and must not ever provide AI tools with personal or sensitive information including photos of current or prior staff or students, names, addresses etc

5. Online Communication and Behaviour

- All online communication must be respectful, courteous, and professional.
- Cyberbullying, harassment, and discrimination are strictly prohibited.
- Users must not engage in offensive or illegal online activities.
- Users must not utilise personal email accounts and platforms for school-related communication or storage of school documents.

6. Content Creation

- Users must respect copyright laws, avoid plagiarism, and not use ICT in any way that impacts on the academic integrity of work produced.
- Using copyrighted materials without permission, such as downloading or sharing music, movies, software, or other copyrighted works without the owner's consent is strictly prohibited.
- Submitting work that is plagiarised is strictly prohibited.
- Users should limit the use of AI tools for the creation of materials for use at The River School and, if using should ensure they use Microsoft CoPilot and not ChatGPT (due to embedded security protocols) and no marketing materials are to use AI generated images
- Users should be mindful of the potential impact of their digital content on others.

7. Network and Internet use

- The school network and internet resources are valuable tools for learning and communication. All users are responsible for using these resources efficiently and prioritising activities that support educational goals.
- Users must be mindful of data download and upload limitations when accessing online content or engaging in network activity, and consider the impact their usage might have on others' access and the overall network performance.
- If users' activities require significant data usage, they should consult with relevant staff to explore options and ensure responsible resource allocation.
- Overloading the network with excessive bandwidth usage, downloading large files for personal use during peak hours, or engaging in activities that disrupt others' access to network resources must be avoided.
- Accessing websites or online services that contain harmful content or present security and privacy concerns is strictly prohibited.
- Using school network resources for personal gain, such as running commercial businesses or engaging in unauthorised online activities is prohibited.

7. Privacy

- Students must not use electronic devices with a camera in any place where a camera would normally be considered inappropriate. This includes in change rooms and toilets or any situation that may cause embarrassment or discomfort to others.
- Students must not invade the privacy of other students or employees of the school by recording (either via photo, video or voice recording) personal conversations or activities without express permission. Any recordings must not be distributed (for example, posting on a social media or website) without express permission. Any such recording or distribution must be done after consent of the relevant person(s) has been expressly and directly gained. Any such recording or distributing without permission will be subject to action under The River School Behaviour Management Policy and to potential police investigation.
- Students must not use an electronic device to bully or cyberbully other students or school employees. Any such behaviour will be subject to action under the *Consequences of Violations* contained in this policy, the Privacy Policy and Privacy Act, and to potential police investigation.

8. Security

- Users should be aware of the risks of online activity and take steps to protect their own data and privacy.
- Users must not collect, store, or share personal information about others without their consent.
- All personal information, including sensitive information, must be handled confidentially and with appropriate security measures to protect against unauthorised access, misuse, or disclosure.
- Users must report potential data breaches or security vulnerabilities in alignment with The River School's Privacy Policy and *Consequences of Violations* section within this policy.
- Students and staff are responsible for the security of their mobile phones and electronic devices.

- The school assumes no responsibility for their loss, theft, or damage of mobile phones and other personal, electronic devices.
- Phones and other electronic devices should be clearly marked with the name of the owner.
- It is strongly advised that students and staff use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones. Students and staff should keep their passwords/pin numbers confidential.
- Mobile phones and other electronic devices that are found at school and whose owners cannot be located are to be handed to the office.

9. STAFF USE OF SCHOOL OWNED ELECTRONIC EQUIPMENT

9.1. Teaching staff may be issued with a school owned laptop or iPad for educational use and limited personal use while an employee at The River School.

9.2. Staff issued, school laptops, or iPads may be taken home provided they are treated with care and respect. The staff member who has been issued the laptop will pay for any repairs resulting from misuse, negligence and undue care.

9.3. Staff are responsible for exercising good judgement regarding appropriate use of school electronic devices. School computers /laptops/iPads must not be used for unlawful, offensive or otherwise improper activities including material that is pornographic, hateful, racist, sexist, abusive, obscene, discriminatory, offensive or threatening to stalk, bully, harass, defame or breach copyright.

9.4. School laptops and iPads are to be used exclusively by the staff member who has been issued the laptop or iPad.

9.5. Upon cessation of employment at The River School, laptops and iPads must be returned in good working order and all personal material removed.

10. RESPONSIBILITIES AND PERSONAL DEVICE USE

10.1. School Responsibilities — The River School acknowledges its responsibility to:

- Develop and implement this policy to ensure the safe and appropriate use of electronic devices by students, parents and employees and ensure the full utilisation of ICT services as essential teaching, learning and business tools with acceptable use parameters
- Communicate this policy to students, parents and employees,
- Keep appropriate records, monitor and report on any issues related to inappropriate electronic device use by students,
- Encourage students, parents and employees to contribute to a healthy school culture.
- Keep a register of staff issued electronic devices, in the school office.

10.2. Personal Device Use

- Personal devices may only be used for school purposes with prior permission and under specific guidelines determined by the school from time to time. A consent form may have to be signed prior to being granted permission to use a personal device, containing an agreement to comply with the specific guidelines and this policy.
- Users are responsible for the security and appropriate use of their personal devices on school premises. The school assumes no responsibility for their loss, theft, or damage.
- Personal device use must not disrupt the learning environment or interfere with school activities.

- Personal devices must not be used to access websites or content prohibited on school technology.
- Recording audio or video with personal devices during school-related activities without the express consent of all individuals involved and in contravention to relevant laws and school policies is strictly prohibited.
- Users must not utilise personal email accounts and platforms for school-related communication or storage of school documents.

10.3. Use of School Identity

- The River School's name, or any images where The River School or The River School students are identifiable, such as students in uniform, may not be used as content to post online without the express permission of the school. This includes but is not limited to posting images or video footage on social media sites.
- Use of social media must not impact the reputation of The River School or any previous/current The River School staff or students.

11. Consequences of Violation

- The River School takes violations of this policy seriously. Misuse of ICT may result in a range of consequences, depending on the severity of the offence.
- Possible consequences may include:
    - Discussions: In some cases, violations may be addressed through discussions about acceptable use with the individual(s) involved and, if appropriate, parents or guardians.
    - Access Restrictions: The school may temporarily or permanently revoke a user's access to the network or limit their access to devices to ensure the safety and security of the school's digital environment.
    - Disciplinary Actions: For more serious violations, the school may take disciplinary actions, such as warnings, suspensions, expulsion, or termination of employment, in accordance with established disciplinary procedures.
    - Legal Consequences: Serious violations that involve illegal activities may also have legal consequences, including potential criminal charges.
- Users must report suspected violations of this policy promptly to the Principal or Deputy Principal.

12. Resources and Support

- The River School will ensure that appropriate information, training, instruction, and supervision is provided to users to enable them to use The River School's ICT assets in accordance with this policy.
- For technical assistance, users may contact the office for IT support.
- Additional resources and information on safe and ethical technology use are available through the office.