

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 Jabiru Community College including school-owned ICT resources as well as personal ICT devices when they are used for school-related activities.	
Scope:	Directors, staff and students. Staff includes: full-time, part-time, permanent, fixed-term and casual employees, as well as contractors, volunteers and people undertaking work experience or vocational placements at Jabiru Community College.	
Status:	Approved	Supersedes: March 2023
Authorised by:	Co-Principals	Date of Authorisation: 2/07/2025
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 • Queensland Government Department of Education Use of ICT systems procedure • Cyber Security Policy • Cyber Security Risk Management Plan • Workplace Bullying Policy • Staff Code of Conduct • Board Code of Conduct Policy All JCC documents are located on Employment Hero or by request	
Review Date:	Every 2 years	Next Review Date: July 2027
Policy Owner:	Co-Principals	

Policy Statement

All Directors, staff and students at Jabiru Community College (JCC) have the right and responsibility to utilise ICT services as essential teaching, learning and business tools. JCC expects this technology to be utilised to its full capacity to provide the most valuable learning and teaching environment to the benefit of all. JCC also expects students and employees to demonstrate acceptable use via safe, lawful and ethical behaviour whenever using ICT services.

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 JCC ICT services are utilised.

JCC reserves the right to restrict employee or student access to ICT services if access and usage requirements are not met or are breached. However, restricted access will not disrupt the provision of the educational program within the school. Employees and students should also note that breaches of this Policy may result in disciplinary action or criminal proceedings.

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.

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, Jabiru Community College 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.

Access and Authorisation

- Access to school technology is granted 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.

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 such as passwords, 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 Jabiru Community College Privacy Policy and Data Breach Response Plan.

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.

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 be mindful of the potential impact of their digital content on others.

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.
- 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.

Personal Device Use

- Personal devices may never be used for school purposes by employed staff.
- 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.

Use of School Identity

- Jabiru Community College's name, or any images where Jabiru Community College or Jabiru Community College students are identifiable, such as students at school 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 Jabiru Community College, or any previous/current Jabiru Community College staff or students.

Consequences of Violation

- Jabiru Community College 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 Co-Principals.

Resources and Support

- Jabiru Community College will ensure that appropriate information, training, instruction, and supervision is provided to users to enable them to use Jabiru Community College's ICT assets in accordance with this policy.
- For technical assistance with Google products, users may contact Geeks on Tap via email: support@geeksontap.com.au or phone: 1300 885 489. Monday- Friday 8am-5pm.
- For technical assistance with Sentral products, users may contact JCC admin staff for assistance or log a job via Sentral portal.
- For technical assistance with Employment Hero products, users may contact JCC admin or Employment Hero through their portal.

Additional resources and information

Responsibilities

School Responsibilities

Jabiru Community College acknowledges its responsibility to:

- develop and implement this Policy to ensure the full utilisation of ICT services as essential teaching, learning and business tools within acceptable use parameters
- communicate this Policy to students, parents and employees
- keep appropriate records, monitor and report on any issues related to inappropriate ICT services
- encourage students, parents and employees to contribute to a healthy school culture.

Employee Responsibilities

At Jabiru Community College employees have a responsibility to:

- uphold the school's Policy on this issue via their own safe, lawful and ethical use of ICT services
- provide guidance and model appropriate behaviour for use of ICT services,
- take reasonable steps to prevent and appropriately respond to any instances of inappropriate use by students of ICT services.

Employee Email Addresses and Phone Numbers

- Staff are provided with an email address and phone number for the purpose of conducting JCC business. They are not to be used for personal purposes.
- JCC issued devices remain the property of JCC and are to be returned to JCC upon the user leaving JCC.
- Personal mobile phone numbers are not to be registered as contact details for conducting JCC business.

JCC Information & Communication Equipment

All staff will be issued with a laptop and a mobile phone. Directors may request to be issued with a laptop if required.

1. Equipment is issued for the purpose of carrying out JCC business. All JCC equipment must be maintained in good order by the user. Users may not install apps or software that is not on the approved whitelist, or without the prior approval of the IT manager.
2. All equipment issued by JCC must be procured through JCC's approved technology suppliers and through existing accounts JCC has with them:
 - a. Office Works;
 - b. Geeks on Tap.
3. If devices are lost or stolen, this must be reported to the Co-Principals immediately.
4. Any notifications or warnings from devices requiring updating must be actioned promptly by the user.

Student Responsibilities

At Jabiru Community College students have a responsibility to:

- uphold the school's Policy on this issue by ensuring the appropriate use of ICT services via safe, lawful and ethical behaviour according to their signed computer use declaration upon enrolment at JCC.
- report any breaches of this Policy to staff.

Implementation

Jabiru Community College will provide students and staff with appropriate training and information as required.

Compliance and Monitoring

Jabiru Community College staff will monitor the use of ICT services as appropriate and record any inappropriate use in the incident register