

1. Purpose

- 1.1 The purpose of this policy is to establish clear guidelines and expectations for the responsible and ethical use of information and communication technology (ICT) by students at John XXIII College.

2. Scope

- 2.1 This policy applies to all students enrolled at John XXIII College who utilise ICT resources provided by the College, whether on campus or remotely. It encompasses all devices, networks, software, and platforms accessed for educational purposes, and extends to any activity involving College ICT resources both during and outside of school hours.

3. Definitions

Information and Communication Technology (ICT): ICT means all computer hardware, software, systems, infrastructure, services and telecommunication devices provided by the College. Additionally, it also includes all parent or personally owned devices used to connect or access the College's technology infrastructure while under the supervision of John XXIII College staff (including, but not limited to, sporting events, excursions, camps and overseas trips).

Wearable recording technologies: Wearable recording technologies include, but are not limited to, smart glasses, AI-enabled glasses, body-worn cameras, wearable microphones, and any device capable of recording, capturing, transmitting, analysing, or storing audio, video, images, conversations, location data, or personal information.

4. Policy Statement

4.1 General Principles

- 4.1.1 The College's ICT resources are predominantly provided for educational purposes. All other use is considered as by exception and is subject to regular review.
- 4.1.2 The College retains the right to withhold access to College ICT resources if students do not comply with the acceptable use of these resources.
- 4.1.3 It is a condition of ICT use that the College reserves the right to inspect all content (e.g. written, graphic, audio, video, email, etc) created, produced, communicated, stored or accessed on all ICT resources or infrastructure (this includes personal devices used under the ICT definition above).
- 4.1.4 It is a priority of the College to increase student awareness of the potential for exposure to inappropriate material and/or potential harm. Students should exercise caution as to the sites they are accessing and the quality and accuracy of the information they are transmitting.

- 4.1.5 As primary educators, parents must be informed of the College policy and support its implementation.
- 4.1.6 This policy shall be made available to the wider College community through the College website, or in a hard copy format upon request.

4.2 Digital Access, Device Usage and Care

- 4.2.1 Student devices provided by the College are the property of the College. Students and a nominated parent/guardian must complete the College-Owned Student Device Agreement (Secondary) or Technologies Student Acceptable Use Agreement (Primary) before a College-owned device will be issued to a student.
- 4.2.2 The College is committed to ensuring that all students are made aware of the fact that unacceptable use of ICT within the College environment will not be tolerated under any circumstances and that disciplinary action will be taken against any student who breaches this policy. The College has identified acceptable and unacceptable uses of ICT:

Acceptable Use	Acceptable use includes, but is not limited to: <ul style="list-style-type: none">• gathering and disseminating appropriate information for educational or related purposes;• working on collaborative projects and resource sharing;• any other tasks that are for educational or related purposes or that support and promote the College and its vision and mission; and• using generative AI tools in accordance with College guidelines, e.g. only using approved platforms and with appropriate supervision and consent where required.
-----------------------	--

Unacceptable Use	Unacceptable use includes, but is not limited to: <ul style="list-style-type: none">• accessing networks without authorisation;• transmitting or deliberately accessing and/or receiving material that is inappropriate or offensive (e.g. threatening, sexually explicit or harassing materials; offensive, defamatory or discriminatory materials; material that may be harmful either physically or emotionally, including bullying or harassment within and outside the College);• being party to, or participating in, acts of harassment, abuse, bullying, threats or behaviour which may be considered capable of causing harm (physical, emotional or psychological) to another student, teacher, staff member or individual within the College community;• any forms of physical or digital vandalism;• knowingly creating and/or introducing viruses or malware;• bypassing the College's network security and/or filtering system, e.g. proxies, tunnelling and/or hotspot access (mobile phone);• removing the College's network connection software, policies, certificates or antivirus software;
-------------------------	---



-
- unauthorised disclosure or communication of information concerning any password, identifying code or other confidential information without permission;
 - interfering with or disrupting network users, services or equipment (e.g. unsolicited advertising; intentional propagation of viruses in any form; using the network to make unauthorised entry to any other machine accessible via the College's network, i.e. 'hacking');
 - wilfully breaching vendor warranty through unauthorised repairs or hacking (e.g. jailbreaking) the operating system, software or applications; and
 - using generative AI tools that are not approved by the College, or using such tools to generate inappropriate, offensive, or misleading content.
-

4.2.6 It is unlawful to use the College's ICT infrastructure and resources to:

- defame someone or an organisation using the College's ICT resources or infrastructure;
- infringe copyright laws, i.e. reproducing or adapting copyrighted material by downloading and further disseminating;
- use ICT in a way that could constitute sexual discrimination or sexual harassment;
- display, store or access sexually offensive or explicit material;
- use ICT in a way that is discriminatory on the basis of race, sex, gender, disability or age, and;
- undertake activities which breach State and Federal legislation.

4.3 Generative AI

4.3.1 Use of generative artificial intelligence (AI) tools must comply with the John XXIII College Generative AI Framework. Students under the age of 13 must not access any large language models (LLMs). Students aged 13 and above may only use College-approved generative AI tools.

4.3.2 Other AI-enhanced tools may be used by students of all ages, provided they are approved by the College and used in accordance with supervision and safety protocols.

4.4 Wearable Recording Technologies

4.4.1 To protect the privacy, safety, wellbeing, and confidentiality of students, staff, and members of the College community, wearable recording technologies are prohibited on College premises, during College activities, and when accessing College ICT systems or information.

4.4.2 Students must not:

- Wear or use wearable recording devices at the College or during College-related activities.
- Record, photograph, livestream, or monitor any person using a wearable device.

- Use wearable devices to access, capture, store, transmit, or process College information.
- Use AI-enabled wearable technologies to record, transcribe, analyse, or share conversations, meetings, lessons, or other College activities.

4.4.3 Any unauthorised use of wearable recording technologies may result in confiscation of the device, restriction of ICT access, disciplinary action, and/or other action in accordance with College policies and procedures.

4.5 Breaches

4.5.1 Unacceptable use of ICT constitutes a serious breach of this policy and possibly the law and may result in a student losing the right to use ICT for a period and/or the application of other sanctions.

4.5.2 Unlawful and/or serious misuse of ICT may result in the College involving the Police or other government agencies.

4.5.3 Emphasis shall be placed on educating students, at a developmentally appropriate level, about ICT, its applications, protocols, abuses and potential dangers. This educative process shall be integrated within all areas of the College curriculum.

4.6 Monitoring and Review

4.6.1 This policy will be reviewed annually, or more frequently pending legislative changes or changes to the College's operations.

5. Roles and Responsibilities

ROLE	RESPONSIBILITY
Director of Inquiry & Innovation and Head of Primary	<ul style="list-style-type: none"> • Maintain this policy to ensure the safe, secure use of ICT by students whilst at the College and using College-owned ICT infrastructure and resources.
Staff	<ul style="list-style-type: none"> • Ensure ICT resources are safe, secure, and monitored. • Teach and model responsible ICT use. • Report and respond to breaches of the policy. • Provide guidance to students on cyber safety and responsible digital citizenship. • Ensure students and their parents/guardians have signed all relevant ICT/device use agreements prior to accessing College-owned ICT infrastructure and resources.
Parents/Guardians	<ul style="list-style-type: none"> • Support the College in implementing the Student Use of ICT Policy. • Encourage safe and respectful online behaviour. • Report concerns about inappropriate ICT use to the College. • Provide consent for ICT access and use of online platforms where appropriate.

6. Information

Title	Student Use of ICT Policy
Relevant Registration Standard(s) and/or Chapter(s)	Standard 5: Premises and facilities Standard 10: Preventing and responding to child abuse Standard 12: Management of students' behaviour Chapter 3: Standard of Education Chapter 4: Levels of Care
Approval date	6 October 2026
Effective date	6 October 2026
Frequency of review	Annually
Review date	6 October 2027
Policy owner	Director of Inquiry & Innovation and Head of Primary
Approving authority	College Executive

7. Related Policy Documents and Supporting Documents

Legislation	Censorship Act 1996 (WA) Copyright Act 1968 (Cth) Crimes Act 1914 (Cth) Criminal Code Act Compilation Act 1913 (WA) Criminal Code Act 1995 (Cth) Defamation Act 2005 (WA) Equal Opportunity Act 1984 (WA) Privacy Act 1988 (Cth) School Education Act 1999 (WA) School Education Regulations 2000 Registration Standards and Other Requirements for Non-Government Schools in Western Australia (2024)
Policies or Frameworks	Australian Framework for Generative AI in Schools John XXIII College Generative AI Framework Staff ICT Use Policy Privacy Policy Privacy Collection Notice
Procedures	N/A
Forms and Templates	College-Owned Student Device Agreement Student Acceptable Use of ICT Agreement (Secondary) Student Acceptable Use of ICT Agreement (Primary) Technology Infringement Notice (Primary)
Other	Student Device Summary Years 4 and 6 College-owned device Years 7, 8 and 9 College-owned device Year 10 Opt-in to the College Owned Device Program Years 10-12 Bring Your Own Designated Device (BYODD)



8. History of Changes

Effective date	Last update date	Policy version no.
1 January 2026	N/A	2026.01
Reviewed policy document to incorporate the College’s Generative AI Framework. This ensures that students are provided with clear guidance regarding the responsible and appropriate use of generative artificial intelligence within the College environment.		
6 October 2026	6 October 2027	2026.02
Amended policy document to incorporate ban on use of wearable recording technologies at the College and during College-related events.		