ICT ACCEPTABLE USE POLICY - STUDENTS

Statement of Context and Purpose

At Huntingtower, we are committed to fostering a safe, respectful and responsible digital environment for students. This policy promotes the responsible and educational use of Information and Communication Technology (ICT) resources, ensuring secure access to these services to enhance students' educational experiences.

Application

This policy applies to all students of Huntingtower. Parents and carers are expected to support their child's safe and responsible use of ICT in line with this policy. Compliance with this policy is essential, along with adherence to the Student Anti-Bullying Policy, the Child Safety and Wellbeing Policy, Child Safety Code of Conduct and Student Mobile Phone Guidelines.

Responsibilities

To ensure a safe and productive digital environment, students are expected to meet the following responsibilities:

- Comply with this policy and each year students and their parents/carers must review and agree to this policy to ensure continued access to School technology resources
- Engage in Digital Citizenship Education, learning about responsible technology use and ethical behaviour online
- Use ICT services only under teacher direction and for learning-related purposes
- Ensure their use of internet (during school hours) and email is teacher-approved and specifically related to their learning
- Follow Bring Your Own Laptop (BYOL) guidelines, including device security, regular software updates and usage restrictions
- Use strong passwords, keep them confidential and change them if compromised
- Log out of shared devices after use and report any suspicious activity (e.g. spam or inappropriate messages) to a teacher
- Acknowledge the original creator or author when publishing or sharing content online
- Recognise that their activity on school systems is monitored and that privacy is limited while using these services
- Act in ways that promote their own wellbeing and that of others when using digital technologies
- Seek explicit teacher permission before using school approved AI tools in learning activities
- Complete tasks substantially on their own and be able to demonstrate personal understanding, even when using AI tools

Prohibited Use

Student must not engage in the following actions which are considered breaches of responsible ICT use:

- Use AI during formal assessments unless clearly permitted in writing by the teacher
- Submit work generated by AI tools without teacher permission or proper acknowledgment

- Upload personal information (e.g. names, photos or videos) into AI tools without explicit consent
- Access social media platforms during school hours, events or activities
- Access, post or distribute content that is sexually explicit, abusive, illegal or defamatory
- Use school ICT systems or accounts to bully, harass, threaten or harm others
- Take or share images or videos of others without their consent
- Log in as or impersonate another user
- Disable or attempt to bypass school virus protection, spam filtering or security settings, including all use of mobile WiFi hotspots, Virtual Private Networks (VPNs) or proxy sites while at school
- Share login credentials or use another person's digital identity
- Download or install unauthorised programs, software or media not directed by a teacher
- Use ICT for unauthorised commercial or personal purposes
- Use the School name or crest without permission from the Principal
- Send emails or messages containing inappropriate attachments, spam, chain letters or confidential content
- Send emails to the entire Year Level without the approval of the Year Level Coordinator or to the whole school without the approval of the Vice Principal

Reporting Incidents

Students and parents must promptly report any suspected or observed incidents of inappropriate ICT use to a Huntingtower staff member and/or the ICT Department.

Cyber Safety & Internet Filtering

The School's ICT Department monitors internet usage to ensure students access appropriate online content. Filtering systems are in place to block inappropriate or harmful material and students must not attempt to bypass or disable these protections. If students or other users encounter unsuitable or concerning material they are expected to report it immediately to a teacher or appropriate staff member. Additionally, if a student experiences or witnesses cyberbullying, they should confide in a teacher or a trusted adult. The definitions and expectations surrounding cyberbullying align with the School's Anti-Bullying Policy.

Cloud Storage and Online Services

To protect privacy and maintain secure access to digital resources, student must follow these practices:

- Microsoft 365, including OneDrive, is provided strictly for learning purposes. Do not upload sensitive, personal or health-related information
- Students must not share login credentials for cloud services and must log out when using shared devices
- Use secure devices and internet connections when accessing resources remotely
- Lessons taught by video conference (such as Microsoft Teams) may be recorded; appropriate behaviour is expected in all online settings
- Students may use Canva AI (Canva Education) for school-related activities across all year levels. Access to ChatGPT is permitted only to students aged 13 years and over. Parental consent is required for the use of both platforms and is obtained through the annual acceptable use agreement. Other AI platforms are strictly prohibited for student use at school.
- All AI use must comply with school policies and platform terms of service

Prevention and Education

Students receive explicit instruction through the integrated curriculum on the safe, ethical and effective use of ICT including the consequences of misuse. Teachers play an active role in reinforcing the School's ICT policies and consistently model responsible digital behaviour in classroom settings.

Classroom teachers regularly clarify expectations around appropriate ICT use which includes using technology as a tool for learning, reporting inappropriate material or misuse, practising responsible email and communication etiquette and seeking help from a trusted adult when facing cyberbullying or digital concerns.

Teachers are also encouraged to address AI-related risks and guide students on appropriate use during their lessons. Through structured programs and consistent messaging, students are supported in developing strong digital literacy skills, resilience and safe online habits. Each student is provided with secure, individual login credentials to access the School's digital systems while internet filters and monitoring tools are used to limit exposure to inappropriate content and track online activity.

Consequences of Misuse

Misuse of ICT resources may lead to consequences such as loss of access privileges, disciplinary action or referral to external authorities. These consequences apply to all members of the School community including students, staff, parents/carers, and volunteers. Failure to acknowledge the use of AI-generated content may be considered plagiarism and a breach of academic integrity. All breaches of this policy will be addressed in line with the School's existing behavioural and academic expectations. In cases of severe misconduct, consequences may include suspension, expulsion or police involvement.

Definitions

- Academic Integrity: The expectation that all work submitted is the student's own, with proper acknowledgement of sources, including AI tools
- Artificial Intelligence (AI): Computer systems or tools capable of performing tasks that typically require human intelligence, such as generating text, images or recommendations
- Generative AI: A type of AI that creates content such as text, images, video or audio often based on user prompts or input
- Community: Includes students, staff, parents/carers, contractors and volunteers who engage with the School's ICT resources
- Cyberbullying: The use of digital technologies to harass, intimidate or cause harm to others
- Digital Citizenship: The responsible, ethical and safe engagement with digital technologies, including respectful communication and data security
- Filtering System: Technology implemented by the School to block access to websites or content deemed inappropriate, unsafe or non-educational
- Hallucination (AI): False or misleading information generated by an AI system and presented as fact
- ICT Resources: Refers to electronic devices, internet services, school network systems, email services and digital tools provided by the School
- Monitoring: The School's practice of tracking activity on its ICT systems to ensure compliance with policies and maintain a safe learning environment
- Personal Devices: Laptops, mobile phones, smartwatches, tablets and any other internet-enabled devices
- Plagiarism: Presenting someone else's work or ideas – including content generated by AI – as one's own without proper acknowledgement

Related documents

- AI Usage Policy
- Student Anti-Bullying Policy
- Child Safety Code of Conduct
- Child Safety and Wellbeing Policy
- Student Mobile Phone Guidelines
- Privacy Policy

- ICT Acceptable Use Policy, Staff
- Child Wellbeing and Safety Act 2005 (Vic)
- Privacy and Data Protection Act 2014 (Vic)
- Crimes Act 1958 (Vic)
- Privacy Act 1988 (Cth)
- Copyright Act 1968 (Cth)
- Enhancing Online Safety Act 2025 (Cth)

Communication

This Policy is available to all staff, students, volunteers, contractors and the School community via the School's website. In addition, relevant aspects of this Policy will be raised at staff and student meetings and highlighted in Bulletins.

Evaluation

The Principal is primarily responsible for monitoring Huntingtower's overall compliance with this Policy, which will be reviewed as part of Huntingtower's policy review cycle (and otherwise as and when required).

Authorisation

This policy was authorised by the Principal April 2015
Reviewed March 2018, April 2020, July 2025
Date of next review: July 2026