

Student ICT Use Policy

1. PURPOSE

Kingswood College recognises its duty to students to maintain a safe physical and online environment for students, as part of its general 'duty of care' obligations, and specifically under Ministerial Order 1359 (clause 13.2 b).

This responsibility is linked to education regarding the safe use of Information and Communication Technologies (ICT) and related Digital Citizenship issues. This policy aims to promote the safety and wellbeing of our students while minimising the opportunity for students to be harmed.

Information and Communication Technologies bring great benefits to teaching and learning programs, and to the effective operation of the College. Students and all members of the Kingswood College community must act ethically and responsibly in their use of technology and social media when such use relates to or may impact on the College or other members of the community.

At Kingswood College, we expect students and all members of our College community to uphold our College values of respect, courage, kindness, perseverance and excellence when engaging with others, which includes their interactions as online digital citizens.

2. SCOPE

This policy applies to all students within the Kingswood College Community.

3. KEY RESPONSIBILITIES

Position/Roles	Responsibilities
College Council	<ul style="list-style-type: none">Ensure the College meets its legal and regulatory responsibilities.Ensure the College meets its duty of care to students
Executive Team	<ul style="list-style-type: none">Establish policy, procedures and guidelines for use of ICT resources and in digital communications.Provide support for staff in undertaking their responsibility in this area
All staff	<ul style="list-style-type: none">Inform students about appropriate and responsible online behaviour
Students	<ul style="list-style-type: none">Uphold the values and ethos of the College in online behaviour

4. KEY ELEMENTS OF THE POLICY

4.1 Definitions

Online Behaviour, for the purposes of this policy, is a general term which includes all behaviour involving the use of communication technology, in terms of the physical technology (including but not limited to

computers, laptops, iPads, phones, etc.) and the various software platforms, web-enabled communication, all forms of social media, and all forms of messaging (containing text and/or images).

Cyber safety refers to the safe and responsible use of information and communication technologies. This includes privacy and information protection, respectful communication and knowing how to get help to deal with online issues.

Common cyber safety issues include but are not limited to:

- cyber bullying;
- sexting (the sending or posting of provocative or sexual photos, messages or videos);
- identity theft or logging in to any device or app as another person; and
- predatory behaviour, where a student is targeted online by a stranger who attempts to arrange a face to face meeting, in an attempt to engage in inappropriate behaviour.

4.2 Kingswood College Policy

Students have the right to learn in a safe environment, including when they have access to ICTs to enhance their learning. Kingswood College is committed to the responsible and educational use of ICTs and to the protection of students by providing secure access to these services as part of their learning experience.

It is our policy that:

- The use of ICTs be managed through a 'whole of College community' approach involving students, staff and parents/guardians/carers; and
- Proactive and reactive ICT education strategies be implemented within the College with a focus on teaching age-appropriate skills and strategies to empower staff, students and parents/guardians/carers to guide appropriate use.

4.3 ICT Misuse Prevention Strategies

Kingswood College recognises that the implementation of whole of College prevention strategies is the most effective way of eliminating, or at least minimising incidents of misuse of ICTs within our community.

The following initiatives form part of our overall ICT strategy:

- A structured curriculum that provides age-appropriate information and skills regarding online behaviour;
- Education, training and professional development of staff;
- The provision of information to parents/guardians/carers to raise awareness of inappropriate online behaviours;
- The promotion of a supportive environment that encourages the development of positive relationships and communication between staff, students and parents/guardians/carers;
- Access to College networks through a filtered service, to restrict access of inappropriate material as well as providing spam and virus protection;
- Students are required to sign and abide by Kingswood College's *Student ICT User Agreement* in order to access the College network (the signed Agreements will be kept). The *Junior School ICT User Agreement* is signed by the student and their parent/guardian/carer, and is age-appropriate;
- A (non-exhaustive) list of inappropriate usage by students is specifically outlined in the *Student ICT User Agreement*;

- The College reserves the right, and uses software to, monitor all content sent and received on the College systems;
- Breaches of acceptable usage of ICTs may result in disciplinary action;
- Risk assessments regarding the inappropriate ICT use within the College are undertaken; and
- Documents supporting appropriate ICT use are included on Compass.

Students whose online behaviour is inappropriate will be managed in accordance with the *Behaviour Management Policy* available on the College's website, and Compass.

4.4 Students use of Mobile Phones at school

Kingswood College acknowledges parents/guardians/carers may wish their child to carry a mobile phone for personal safety reasons however, the right of a student to have access to a mobile phone at school must be balanced with the responsibility to use it appropriately.

It is our policy that:

- Mobile phones are brought to school at the owner's own risk. No liability will be accepted by the school in the event of loss, theft or damage of the phone;
- Mobile phones must be kept in locked lockers during the school day, and not accessed at all during the school day;
- Mobile phones may only be used by students in classrooms for a specific learning activity with permission from their teacher;
- Staff should be alerted and exceptions requested if a student has special circumstances requiring the use of their mobile phone during school hours (e.g. health issues);
- Mobile phones must not be brought into exams or class assessments (even if they are turned off or on silent mode);
- Phone cameras are not to be used within the school grounds where it would be considered inappropriate such as in change rooms or toilets;
- Students should never photograph or record any person without their express permission;
- Reports of incidents of misuse of mobile phones will be recorded and retained on the student's file; and
- Parents/guardians/carers are to be informed that in cases of emergency, the school remains an appropriate point of contact to reach their child quickly (by contacting the relevant school administration).

4.5 Privacy Risks

To protect their privacy online, students are advised to:

- Personally regularly review and adjust the privacy settings on their social media pages
- Only add people that they know and trust as online friends and contacts
- Protect their accounts with strong passwords
- Not access social media sites by clicking a link provided in an email or on another website
- Disable 'geo-tagging' or location information sharing on social media accounts and mobile devices to prevent strangers from knowing their personal home or College locations;
- Limit the amount of personal information (e.g. date of birth, address, information about your daily routine, holiday plans etc.) they provide on social media sites to prevent identity crime.

4.6 Sexting

Sexting is the sending or posting of provocative or sexual photos, messages or videos online. Sexting will generally constitute criminal conduct when it involves students aged under 18 and when it involves harassment or bullying. The creation and/or distribution of the images may constitute child pornography. Where sexting involves minors, the Police will be notified.

4.7 Our Wellbeing team

The Wellbeing team will:

- Review the school's *Student ICT Use Policy*, *Student ICT User Agreement*, and *Junior School ICT User Agreement* as required;
- Plan relevant cyber safety initiatives (such as student education, staff professional development, parent/guardian/carer information) to minimise the risk of inappropriate online behaviour;
- Maintain an awareness of cyber safety best practice for schools;
- Review and analyse data obtained from any school surveys that deal with cyber safety issues;
- Make recommendations to the Principal with respect to improvements to the school's ICT and cyber safety policies and procedures; and
- Act as primary point of contact for cyber safety related issues that may arise during the year.

4.8 Staff Responsibility

Teaching staff are expected to:

- Ensure all students are: provided with a *Student ICT User Agreement* (or *Junior School ICT User Agreement*, as applicable) which is explained in an age-appropriate way; and warned that consequences for inappropriate behaviour will be managed in accordance with our *Behaviour Management Policy*;
- Be vigilant in monitoring students when using ICT equipment and devices;
- Reinforce to students the importance of privacy and safeguarding their login details, personal information and the personal information of others;
- Assist students in the event that they have inadvertently accessed inappropriate material, received inappropriate messages or if they have been offended by another person's use of ICTs;
- Report any observed incidents of inappropriate ICT use in accordance with this policy; and
- Ensure that any incident of inappropriate ICT use that they observe or is reported to them, is recorded appropriately.

4.9 Implementation

This policy is implemented through a combination of:

- Staff training;
- Student and parent/guardian/carer education and information;
- *Student ICT User Agreement* (or *Junior School ICT User Agreement*, as applicable);
- Effective student supervision;
- Effective monitoring as part of the College networks;
- Effective incident reporting procedures;
- Effective management of incidents of inappropriate ICT usage when reported and/or observed;

- Effective record keeping procedures; and
- Initiation of corrective actions where necessary.

4.10 Breach of Policy

A breach of this Policy, or the *Student ICT User Agreement* (or *Junior School ICT User Agreement*, as applicable), may also involve a breach of other College policies, and should be managed in conjunction with the College *Behaviour Management Policy* and *Respectful and Safe School Policy and Guidelines*.

All reports of inappropriate online behaviour, including cyber bullying, hacking and other technology misuses, will be investigated and may result in a notification to Police.

Sanctions for students may include, but are not limited to, the loss of ICT privileges, suspension, or expulsion from the College.

Students and parents/guardians/carers must be aware that in certain circumstances where a crime has been committed, they may be subject to a criminal investigation by Police over which the College will have no control. The College will cooperate fully with any Policy investigation.

5. RELATED POLICIES AND DOCUMENTS

Student ICT User Agreement

Behaviour Management Policy

Respectful and Safe School Policy and Guidelines

Junior School ICT User Agreement

6. REFERENCES

Complispace Template Policy documents relating to: ICT, Cyber Safety, Social Media and Use of Mobile Phones