ICT Use Policy

Hills
Grammar

Hills Grammar

ICT Use Policy

Approval and Review	Details
Document Owner	Director of ICT
Responsibility	Director of ICT / Deputy Principal
Approver	Principal
Issue Date	June 2022
Reviewed	June 2023 | June 2024
Next review date	June 2025

Purpose

At Hills Grammar the use of Information and Communication Technologies (ICT) aims to enhance the effectiveness of the learning and work environment. The use of ICT facilities must be in accord with the School's values, Student Management and Behaviour Policy, Community Code of Conduct, Mobile Phone Policy, Privacy Policy, AI Guidelines and Staff Code of Conduct.

The purpose of this policy is to provide the School's guidelines and expectations for the acceptable use of ICT.

Scope

These guidelines and expectations apply to all Hills Grammar students, staff, member of School Council, contractors and guests who may make use of the School's ICT facilities and network. This policy applies to the use of ICT resources supplied by the school as well as the use of technology owned by the individual whilst at school or participating in school activities, or when communicating with any member of the school community.

Definitions

Information Communication Technologies are any electronic device or related applications which allows users to record, send, access, or receive information in textual, audio, image, or video form. These may include but is not restricted to:

- Computer systems including personal computers, laptops, and tablets
- Related applications such as email, Internet, and Learning Management Systems
- Discussion forums, chat rooms, social media, and instant messaging systems (such as SMS and MSN)
- Mobile phones, PDA's and iPods, iPads and any other portable devices
- Digital storage devices
- Fax and scanning devices
- Video and still cameras
- Audio recording devices

Devices and applications are provided by the School for access to information – this includes wired and wireless network access points that are monitored and filtered. Students are expected to follow these School guidelines and expectations when using school issued devices and applications, as well as when using their own devices under the BYOD program.

A user is any person who has been granted access to the School's ICT facilities. This can include students, staff, contractors, members of School Council, student teachers, external tutors, and guests to the School.

Guidelines and Expectations

Use of ICT

The School's ICT network and facilities are an educational and business facility provided by the School primarily for educational and business purposes. Students are to use these resources to enhance, enrich and extend their learning opportunities. Staff have responsibility to use the resources in an appropriate, ethical, lawful, and professional manner.

All email and internet-based messages systems on the School's network will be treated as being made for educational and / or business purposes. Accordingly, all communications should be considered to be non-private.

Staff are permitted to use the School's ICT facilities for appropriate personal use, provided that such use is kept to a minimum, is made in accordance with the School's Staff Code of Conduct, and does not interfere with the staff member's responsibilities, and duties or with the effective and efficient operation of the School. However, all communications made through the School's ICT facilities are subject to the same terms and conditions as described in this policy.

Users are often able to access communications technologies through their own providers (mobile phone and mobile internet) while at school. Students are expected to follow School guidelines and expectations when using their own devices and providers in the school context. While at school students are required to use the school provided WiFi for internet access from their laptops. At no time are they permitted to use mobile hotspots to access the internet on laptops.

The School does not accept liability for personal items of information and communication technologies brought on to the School grounds by members of the community. However, the School reserves the right to manage the use of technologies within the school community.

Appropriate Use of email and other internet communications

All ICT communications are not private nor secret and individuals may be accountable for what is written, said, or transmitted in an ICT message. Messages may be easily copied, forwarded, saved, intercepted, archived and may be subject to discovery for legal purposes. The audience of a message may be unexpected and widespread.

The School's ICT facilities must not be used:

- to abuse vilify, defame, harass, degrade, or discriminate (by virtue of sex, sexual orientation, race, disability, religion, ethnicity or other).
- to send, receive or store what would be reasonably considered obscene, offensive, or pornographic material.
- to discuss or comment on the physical appearance of other persons (regardless of whether the message was sent to the person in question).
- to injure the reputation of the School, to cause embarrassment to the School or its students, staff, or Council.
- to send information for the purpose of causing damage to the School's ICT facilities, such as spam emails, viruses etc.

- to infringe the copyright or intellectual property rights of individuals or organisations.
- to perform any other unlawful or inappropriate conduct act.

In instances where a staff member or student inadvertently accesses inappropriate material this should be brought to the attention of the Principal or their delegate in order for appropriate actions to be taken to protect others.

Email Etiquette

Email is a useful communication tool, but care must be taken to ensure its use is appropriate and effective. The following points act as a guide for the appropriate use of email:

- Email is an education / business communication and should be written accordingly.
- Emails should contain a clear subject line providing a clear indication of the purpose of the email.
- For staff and student emails should only be sent from Hills Grammar accounts.
- An email should have a salutation that is appropriate for the relationship you have with the recipient.
- Be cautious of the “reply all” function. Before using this consider whether all other recipients need to have your reply. For example, if you are simply thanking the sender then using the reply all function creates unnecessary emails for others.
- The blind copy function (BCC) is only to be used when sending bulk emails where others should not have access to email addresses, such as when emailing a group of parents. Under no circumstances should the BCC function be used to avoid the recipient knowing the email has been sent to others.
- Tone is difficult to gauge in an email so consider language carefully and if in doubt perhaps consider phoning the recipient or meeting them in person.
- Except in exceptional circumstances avoid sending emails after 6pm or on weekends. Make use of the delay delivery function if drafting emails out of these hours.

Monitoring

The contents and usage of email, other internet communications and internet usage made on the School’s ICT facilities may be subject to regular random monitoring by the School or by a third party on the School’s behalf. This may include electronic communications which are sent and / or received internally or externally. Where inappropriate use is reasonably suspected the Principal may authorise the School’s ICT personnel to examine a user’s web-access logs, email accounts or other internet communications.

The School also reserves the right to audit any material stored or accessed on equipment that is owned or leased by the School and to audit any privately owned devices, including storage devices, used at the School or at a school related activity.

No monitoring will occur without the express permission of the Principal with the exception of normal logging of system usage to manage the network.

Safety and Security

Passwords

All staff and students will be issued with a unique username and password to access the School's ICT facilities. Passwords must:

- be kept secured and not shared with others. ICT personnel are not to ask a person for their password, even for the purpose of providing assistance.
- be made strong and are not to be the same as those used for non-school purposes
- be reset when required by the ICT Department
- be reset from generic passwords initially issued by the ICT Department.

In the event that a student or staff member becomes aware that their password has been compromised they should immediately notify the ICT Department to have the password reset.

Access to information

Except in circumstances related to monitoring as outlined above no users are permitted to access another users' digital files or communications. In the event of there being a legitimate business reason for accessing information, such as access to a former staff members file, access may only be granted with the written consent of the Principal. This will outline the specific information to be accessed, the persons who are to have access and their reasons access being granted.

Personal Safety

The safety and wellbeing of all members of the School community is important. Disclosure of personal information can expose users to inappropriate and / or unwanted material and commercial solicitations, physical danger, financial risks, exposure to unreliable information, bullying and harassment and identity theft. Consequently, it is important that user do not send or post personal information to unknown or dubious sources. This includes information such as home addresses, phone numbers, email addresses, dates of birth etc.

When using digital resources with students Hills Grammar staff will take additional care to minimise this risk to students through educative processes.

Digital Citizenship

When accessing and communicating via the School's ICT facilities all users are expected to demonstrate the School's values, most particularly the values of Respect and Integrity.

Instances of cyber-bullying, online harassment or discrimination directed towards a member of the School community by a student or staff member will not be tolerated and will be managed in accordance with the School's Student Management and Behaviour Policy or Staff Code of Conduct. Staff and students who become aware of such activities are expected to report them appropriately to the Principal or their delegate. Similarly, students or staff who engage in such activities towards others in the wider community may be considered to be not expressing the School values and may be subject to action under appropriate School policies.

Using School's ICT facilities to capture, store, send, forward or receive images of a sexual nature, regardless of consent, is not permitted under any circumstances and will be dealt with in accordance with the appropriate School policy. Such activities may also constitute a criminal act and may be reported to the police for further action. Where such images are received by a user in an unsolicited fashion through the School's ICT facilities, the user must report the incident immediately to the Principal for further investigation.

When using and accessing digital resources staff and students must consider the intellectual property rights of others and ensure that their use is in accordance with the appropriate copyrighted uses. If there is doubt, then staff and students are not to copy or use resources that may infringe such copyright. Instances of plagiarism, this involves taking the ideas or work of others and presenting them as your own original work or ideas, may result in a student being in breach of the School's assessment guidelines and may also result in them facing sanctions regarding their access to the School's ICT facilities. The acceptable use of AI is outlined in the School's AI Guidelines.

Good digital citizenship also involves respecting the privacy of others. Respecting other people's privacy includes:

- Not forwarding or reposting messages that have been sent with the intent that they are private.
- not taking or sharing photos, sound, or audio recordings of others without their permission; and
- Not distributing personal information about others, such as mobile phone numbers, without permission

When using digital resources with students Hills Grammar staff will take additional care to minimise this risk to students through educative processes.

Illegal and Disruptive Activities

Users of the School's ICT facilities are subject to laws governing the use of electronic devices and communications. Users must not:

- attempt to gain access to any service or network system to which they do not have authority to access. This includes logging in, or attempting to log-in, using another person's username and password.
- deliberately attempt to disrupt another person's access to the School's ICT facilities.
- deliberately attempt to destroy data through unauthorized access, spreading a digital virus or by other means.
- install, or attempt to install, software which is harmful to the School's ICT facilities or for which the school is not licenced.
- attempt to circumvent measures put in place by the School to protect its ICT facilities, data, or the privacy of other users.
- attempt to circumvent the School's internet filtering systems, including the use of mobile hotspots; and
- engage in act that is illegal, including the use of the School's ICT facilities to access sites deemed illegal, to purchase products of an illegal or inappropriate nature, threaten or harass another person

Instances of illegal activity will be reported to the police for further investigation.

Cybersecurity measures

The School has the following Cyber Security measures in place for students and staff:

- A Paloalto nextGen Firewall that ensures that staff and students can only access appropriate content and resources on the Internet, while also protecting our internal network from malicious attack from outside. The firewall also provides tools for monitoring and alerting around Internet usage and potential attack activity.
- All Internet access by staff and students is logged and monitored.
- Saasyan used to monitor student Internet usage, including emails and Microsoft Teams chats for inappropriate and antisocial behaviour, bullying, indicators of risk of self-harm and other wellbeing related issues.
- Microsoft Defender, an anti-virus/anti malware solution, on all staff and student school owned laptops.
- The internal network is configured with vlan segregation, where every year group has its own vlan to reduce the attack surface and prevent sideways movement within the network should a hacker be able to compromise a single device.
- We require complex passwords for all students and staff accounts and enforce changing these passwords periodically.

- Office 365 Malware protection is enabled on all our email communications. This provides a tool to reduce SPAM and also block malicious email from reaching staff and students.
- Periodically we conduct simulated Phishing attacks in order to better educate staff on how to spot a fraudulent and potentially harmful email.
- Staff and student laptops have Defender for Office 365, which includes tools such as ATP Safe Links, monitors email for links that may lead to potentially harmful downloads and websites.
- Microsoft A5 licensing, provides a range of tools to further protect our staff and students by using AI to monitor login behaviour and detect potential risky signins and other risky user behaviour.
- Staff accounts are protected with Multi Factor Authentication (MFA).

Student Expectations

Students are expected to abide by the measures that are outlined in this policy. Furthermore, they should:

- Be safe, responsible, and respectful users of technology and online services.
- Respect and follow school rules and procedures and the decisions made by staff and the School
- Always act with integrity when using digital devices and understand the impact of their digital footprint in the present and the future.
- Communicate respectfully and collaboratively with peers, school staff and the school community and behave in the ways described in the Behaviour Management Policy and the Student Relationship Policy.
- Respect and protect the privacy, safety, and wellbeing of others.
- Not share anyone else's personal information.
- Not take or share a photograph or video of someone without permission.
- Not harass or bully other students, school staff or anyone, using a digital device or an online service.
- Not send or share messages or content that could cause harm.

Staff Expectations

All staff are expected to abide by the measures outlines in this policy. Furthermore, they should:

- Support, encourage and expect safe, responsible, and respectful use of technology and online services. This includes:
    - Establishing and upholding agreed classroom expectations for using technology and online services.
    - Following the school's behaviour management plan when responding to any incident of inappropriate student behaviour relating to the use of digital technology or online services.
    - Understanding the rules and regulations associated with the use of technology and online platforms, such as age limitations.
    - Educating students about online privacy, intellectual property, copyright, digital literacy, and other online safety related issues.
- Model appropriate use of technology and online services.
- Respond to and report any breaches and incidents of inappropriate use of technology and online services as required by school procedures and any statutory and regulatory requirements.
- Participate in professional development related to appropriate use of digital devices and online services.

Parent and Carer Expectations

Parents and carers should:

- Recognise the role they play in educating their children and modelling the behaviours that underpin the safe, responsible, and respectful use of technology and online services.
- Support implementation of the school procedure, including its approach to resolving issues.
- Take responsibility for their child's use of technology and online services at home such as use of online services with age and content restrictions.
- Communicate with school staff and the school community respectfully and collaboratively as outlined in the Parent Communications Policy and Parent Code of Conduct Policy.
- Switch off or put their digital devices on silent when at official school functions, during meetings and when assisting in the classroom.

Development of a Whole School Approach to Technology Use

Safe use of technology and online safety are underpinned by an effective whole-school approach for promoting student wellbeing and preventing student harm. Our approach at Hills is to empower students to participate meaningfully in the design, development, and implementation of their safe use of technology and online safety. The Student Wellbeing Team performs a key role in the development of our ICT Policy and Mobile Phone Policy.

Breach of Acceptable Use

Users who fail to abide by the acceptable use of ICT resources will have consequences applied that may include having their access to the School's ICT facilitated restricted. In serious cases breaches will be dealt with in accordance with the School's K-12 Student Management and Behaviour Policy or Staff Code of Conduct. Where illegal activities are suspected matters will be referred to the police or other appropriate authorities. Everything done on the school's network is monitored and can be used in investigations, court proceedings or for other legal reasons.

eSafety

Our School acknowledges that the eSafety Commission provides excellent resources for parents, carers, students, and staff regarding online safety – https://www.esafety.gov.au/educators