GEELONG GRAMMAR SCHOOL®
| Exceptional Education |

CYBERSAFETY POLICY

STAFF

Instructions for Staff

Read this document and if there are any points you would like to discuss with the School, let the Head of Campus know as soon as possible.

Definition of terms used in this Policy:

(a) 'Authorised User' means an employee who is authorised by the School to use School ICT.

(b) 'Cybersafety' refers to the safe use of the Internet, social media, and ICT equipment/devices, including mobile phones.

(c) 'Electronic communication' includes, but is not limited to, communication made by using ICT equipment/devices such as Internet, Intranet, Email, Social Media and mobile phone activities and related applications.

(d) 'ICT' means the term 'Information and Communication Technologies'.

(e) 'ICT equipment/devices' includes, but is not limited to, computers (such as desktops, laptops\notebooks, PDA"s), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players, external hard drives), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies as they come into use.

(f) 'Objectionable' means material that deals with matters such as sex, cruelty, violence, gambling or terrorism in such a manner that it is likely to be injurious to the good of students or incompatible with a school environment.

(g) 'Policy' means this Policy and incorporates any related Cybersafety policy which may be developed by the School from time to time.

(h) 'Prohibited use' means use of School ICT or privately owned or leased ICT on the School site or at any School-related Activity, in a manner which is contrary to the terms of this Policy and includes, but is not limited to, conduct specified in paragraph 2.4 of this Policy.

(i) 'School' means the Geelong Grammar School (all campuses).

(j) 'School-related activity' includes, but is not limited to, a field trip, camp, sporting or cultural event, wherever its location.

(k) 'School ICT' means the School's ICT and ICT equipment, devices and network.

(l) 'Social Media' includes, but is not limited to:

- Multimedia and social networking websites;
- Blogs; and
- Wikis.

(m) 'Unacceptable use' includes, but is not limited to, acts of a malicious or nuisance nature, invasion of privacy, harassment, bullying, hacking, altering the settings on any ICT device or equipment without authorisation, plagiarism, gaming, impersonation/identity theft, inappropriate use of Email and distribution of unacceptable material, spoofing, gambling, fraud, copyright infringement, or cheating in an examination.

INTRODUCTION

The values promoted by Geelong Grammar School include respect for self, respect for others in the School community, a commitment to enabling everyone to achieve their personal best in an environment which is physically and emotionally safe and kindness towards all. The School has a zero tolerance approach to child abuse and any threat to the safety of a child will be treated seriously as detailed in the Child Safety Policy. The measures to ensure the Cybersafety of the School environment which are outlined in this Policy are based on these core values.

The School's computer network, Internet access facilities, computers and other School ICT equipment/devices, together with privately owned or leased ICT equipment used in the School environment, extend significant benefits to the teaching and learning programmes at the School, and to the effective operation of the School. Within this context, the objective of this Policy is to ensure the safe use of ICT within the School community.

This Policy includes information about scope of application, obligations, responsibilities and the nature of possible consequences associated with breaches of the Policy. The overall goal of the School is to provide an educative environment with the objective of establishing a Cybersafety culture which is in keeping with the values of the School, legislative and professional obligations and the community's expectations.

This Policy specifies the conditions applying to the use of the electronic communication system at the School. Electronic communications include, but are not limited to, all Internet, Intranet and Email activities and related applications. Authorised Users of the School's electronic communication systems are required to comply with the Policy. Failure to observe and abide by this Policy may result in disciplinary action.

Breaches of this Policy can undermine the values of the School and the safety of the learning environment, especially when ICT is used to facilitate misconduct. Such a breach which is deemed by the School at its sole discretion to be harmful to the safety of the School (for example, involvement with inappropriate or objectionable material, or anti-social activities like harassment and/or bullying), may constitute a significant breach of discipline and possibly result in serious consequences.

SCOPE OF STAFF POLICY

This Policy applies to all School staff (teaching, non-teaching and trainee), whether part-time, full-time, casual or relieving, and whether or not they make use of the School network, Internet access facilities, computers, staff laptops and other School ICT equipment/devices. Although some staff may not have any teaching or supervisory responsibilities with students, as members of the School community they need to be aware of measures to help ensure Cybersafety.

USER CYBERSAFETY OBLIGATIONS

1 Authorised Usage and Cybersafety Policy

1.1. Authorised Users may use School ICT for electronic communication for School business and educational purposes. Where necessary, use of School ICT for personal purposes may be allowed at the sole discretion of the School, provided such use does not contravene this Policy or have any negative ramifications for the School and does not adversely impact upon work productivity and professional standards.

1.2. As the School provides access to School ICT, the contents of the School ICT systems remain the intellectual property of the School. The School has the capacity to monitor and control its ICT system and reserves the right to monitor individual usage and report, where necessary, any indications of misconduct or prohibited use.

1.3. This policy will be made available on the Portal to all users, whether or not they make use of the School's computer network, Internet access facilities, computers and other ICT equipment/devices in the School environment.

1.4. The School encourages anyone with a query about the Policy to contact the Head of Campus, as soon as possible.

2 Obligations and requirements regarding appropriate use of ICT in the School learning environment

2.1. The use of the School's computer network, Internet access facilities, computers and other School ICT equipment/devices or software, on or off the School site, is for both educational and personal use given the nature of the School environment. This applies whether or not the ICT equipment is privately owned or leased.

2.2. The use of any privately-owned or leased ICT equipment/devices on the School site, or at any School-related activity must be appropriate to the School environment. This includes any images or material present/stored on privately-owned or leased ICT equipment/devices brought onto the School site, or to any School-related activity. Such ICT equipment/devices could include a laptop, notebook, desktop, PDA, mobile phone, camera, recording device, or portable storage (like a USB or flash memory device). Anyone unsure about whether or not it is appropriate to have a particular ICT device at School or at a School-related activity, or unsure about whether the planned use of a particular ICT device is appropriate, must check with the Head of Campus. Any ICT device which requires connectivity to the school network will require approval from the ICT Manager.

2.3. When using the School's ICT systems, the School will monitor and control network activity and may use appropriate devices to filter or screen material. In the light of this possibility Authorised Users are required to make responsible use of the system at all times.

2.4. When using School ICT, or privately-owned or leased ICT on the School site or at any School-related activity, prohibited use includes, but is not limited to, any conduct that:

- Violates or infringes the rights of any other person, including the right to privacy.
- Initiates access to objectionable, inappropriate or illegal material.
- Initiates access to material which contains actual or potentially defamatory, false, inaccurate, abusive, obscene, violent, pornographic, profane, sexually-explicit, sexually-oriented, threatening, racially offensive or otherwise biased, discriminatory or illegal or any other objectionable or inappropriate material.
- Violates any other School policy, including prohibitions against harassment of any kind.
- Forwards confidential messages to persons to whom transmission was never authorised by the School, including persons within the School community and persons/organisations outside the School community.
- Broadcasts unsolicited personal views on any matter
- Fails to use the School's ICT system as prescribed, thus permitting infection by computer virus or deliberate infection by computer virus.
- Attempts to access personal data by using or attempting to use a password not specifically allocated to the authorised user.
- Involves sharing of copyright material e.g. music or software.
- Attempts to breach security and infrastructure that is in place to protect user safety and privacy.
- Involves the establishment or conduct of personal or private commercial or business transactions.
- Propagates chain emails or uses groups or lists inappropriately to disseminate information.
- Results in unauthorised external access to the School's electronic communication system.
- Inhibits the authorised user's ability to perform their duties productively and without unnecessary interruption.
- Interferes with the ability of others to conduct the business of the School.
- Involves the unauthorised installation and/or downloading of non-School endorsed software.
- Involves malicious activity resulting in damage to School ICT and/or ICT equipment/devices.
- Offends or potentially offends the ethos, principles and/or foundations of the School.

In the event of accidental access of such material, Authorised Users must:

- Not show others
- Close or minimise the window
- Report the incident immediately to the Head of Campus

2.5. A person who encourages, participates or otherwise knowingly acquiesces in prohibited use of School ICT, or privately-owned or leased ICT on the School site or at any School-related activity, may also be found to have engaged in prohibited use.

2.6. Under no circumstances should ICT be used to facilitate behaviour which is either inappropriate in the School environment or illegal.

2.7. To avoid any doubt, this Policy also applies to communication devices including mobile phones. Mobile phones must not be used for involvement with objectionable or inappropriate material or activities, such as:

- Upsetting or harassing fellow co-workers, students, School management or persons in the community.
- Inappropriately using text, email photographs or film, phone messages, audio recordings, web browsing, images or any other functions.

2.8. While at School or a School-related activity, Authorised Users must not have involvement with any material or activity which might put them at risk. In addition, Authorised Users must not at any time use ICT to upset, harass, stalk or harm anyone.

2.9. Authorised Users must not attempt to download, install or connect any unauthorised software or hardware onto School ICT equipment, or utilise such software/hardware. This includes use of such technologies as Bluetooth, infrared, and wireless, and any other similar technologies that are available. Any Authorised Users with a query or a concern about that issue must speak with the Head of Campus.

2.10. In a special case where permission has been given by the Head of Campus to connect or install privately-owned ICT equipment/devices or software, it is with the understanding that the School may scan this ICT equipment/device/software at any time thereafter as part of a regular or targeted security check, such as for viruses.

2.11. When using Social Media on school ICT, or privately-owned or leased ICT whether on the School site or otherwise, Authorised Users must not post or link to any information or material that is:

- Confidential or proprietary information relating to the School or its students;
- Personal information of others, even if the other person consents or agrees;
- Obscene, indecent, defamatory, objectionable, inappropriate, threatening, harassing, discriminatory or hateful to the School, any of the School's staff or students or anyone else in the community.

2.12. The Authorised Users' obligations pursuant to clause 2.11 of this Policy extend to the use of ICT outside of ordinary School hours and regardless of whether the use occurs on School site, at a School-related activity or otherwise.

2.13. Any breach of clause 2.11 of the Policy whether inadvertent or deliberate will result in disciplinary action being taken by the School against the perpetrator which may include termination of employment.

2.14. The principles of the School's discrimination, harassment and equal opportunity policies apply equally online and when using ICT as in all other areas.

3 Additional staff obligations

3.1. To the best of their ability, School staff are responsible for ensuring the safety and wellbeing of students using School ICT and privately owned or leased ICT or ICT equipment/ devices on the School site or at any School-related Activity.

3.2. School staff must:

- Guide students in effective strategies for searching and using the Internet and ICT; and
- Actively supervise students when they are accessing the Internet in a classroom situation or School-related activity.

3.3. To the best of their ability, staff must support, encourage and facilitate students' compliance with the Student Policy, including:

- Endeavouring to ensure all students in their care understand the requirements of the Student Policy, especially very young students, students who are newly enrolled at the School, students for whom English is a second language, and students with special needs; and

- Regularly reminding students of the contents of the Student Policy and encouraging them to make positive use of ICT and to notify School staff if the student becomes aware of a potential breach of the Policy or is seeking support in this regard.

3.4. Staff obligations in respect to confidentiality and privacy extend to cover information relating to other staff and/or students and their families which is stored on School ICT and which is accessed or inadvertently viewed by a staff member.

3.5. Staff members (including Assistants) may not be included as a "personal friend" on a student's social networking page (e.g. Facebook) and vice versa. The School policy regarding this is:

- Staff cannot invite current students to be a "personal friend' on social networking sites

- Staff cannot accept invitations from current students to be a "personal friend" on social networking sites

- Staff wishing to use social media in the course of their school duties must create a separate professional account.

- Only Closed Facebook Groups are permitted for educational use and they must be set up and managed using a professional account.

3.6. To avoid any breach of privacy laws, staff members must seek advice from the School's senior management when appropriate in relation to matters such as the collection of images, privacy, safety and copyright associated with student material.

3.7. Staff must report any incidents involving Cybersafety issues of which they become aware to the Head of Campus or his/her designated representative as soon as reasonably possible.

3.8. Upon becoming aware of an incident involving suspected prohibited use or illegal use of School ICT, or privately-owned or leased ICT relating to the School or any student or fellow staff member of the School in any way, whether by a student or another member of staff, staff must immediately report the incident to the Head of Campus.

4 Monitoring by the School

The School:

4.1. Reserves the right at any time to check work or data on the School's computer network, Internet access facilities, computers and other School ICT equipment/devices without obtaining prior consent from the relevant Authorised User. For example, teachers may at any time check student email or work.

4.2. Reserves the right at any time to check work or data on privately-owned or leased ICT equipment on the School site or at any School-related activity. The Authorised User agrees to promptly make the ICT equipment/device available to the School for the purposes of any such check and to otherwise co-operate with the School in the process. Before commencing the check, the School will inform the Authorised User of the purpose of the check.

4.3. Has several electronic access monitoring systems which have the capability to record email and Internet use, including the user details, time, date, sites visited, length of time viewed, and from which computer or device.

4.4. Monitors traffic and material sent and received using the School's ICT infrastructures. From time to time this may be examined and analysed to help maintain a Cybersafe School environment.

4.5. May deploy filtering and/or monitoring software where appropriate to restrict access to certain sites and data, including email.

4.6. Will clearly indicate that during the logon process that Staff, by logging on, are bound by the School ICT policies.

4.7. May from time to time conduct an internal audit of its computer network, Internet access facilities, computers and other School ICT equipment/devices, or may commission an independent audit of content and usage.

5 Copyright, Licensing and Publication

5.1. Copyright laws and licensing agreements must be respected and sources appropriately acknowledged. Authorised Users must not be involved in any activity which may breach copyright laws and licensing agreements including, but not limited to, activities such as illegally copying material in any format, copying software, downloading copyrighted video or audio files, using material accessed on the Internet in order to plagiarise, or illegally using unlicensed products.

5.2. All material submitted for internal publication should be appropriate to the School environment.

5.3. All material submitted for external publication should appropriately represent the School environment and be approved by the School prior to publication.

6 Individual password logons to user accounts

6.1. If access is required to the School computer network, computers and Internet access using School facilities, it is necessary to obtain a personal user account from the School.

6.2. Authorised Users must keep passwords confidential and not share them with anyone else. A breach of this rule could lead to Authorised Users being denied access to the School ICT system.

6.3. Authorised Users must not allow another person access to any equipment/devices logged in under their own user account, unless with special permission from the Head of Campus. Material accessed on a user account is the responsibility of that Authorised User. Any inappropriate or illegal use of the computer facilities and other School ICT equipment/devices can be traced by means of this logon information.

6.4. Those provided with individual, class or group e-mail accounts must use them in a responsible manner and in accordance with this Policy. This includes ensuring that no electronic communication could cause offence to others or harass or harm them, put the owner of the user account at potential risk, contain objectionable material or in any other way be inappropriate in the School environment.

6.5. For personal safety and having regard to Privacy laws, Authorised Users must not reveal personal information about themselves or others. Personal information may include, but is not limited to, home or email addresses, and any telephone numbers, including mobile numbers.

7 Other Authorised User obligations

Authorised Users must be considerate and must:

7.1. Ensure private usage of School technology resources including mobile phones is fair and reasonable.

7.2. Avoid involvement in any incident in which ICT is used to send or display electronic communication which might cause offence to others and/ or involve objectionable material.

7.3. Not display or send objectionable and/ or inappropriate graphics, and/ or record or play objectionable and/ or inappropriate audio or video files.

7.4. Abide by copyright laws and obtain permission from the individual before photographing, videoing, or recording them.

8 Privacy

8.1. School ICT and electronic communication should not be used to disclose personal information of another except in accordance with the School's Privacy Policy or with proper authorisation. The Privacy Act requires the School to take reasonable steps to protect the personal information that is held by the School from misuse and unauthorised access. Authorised Users must take responsibility for the security of their ICT equipment/devices and not allow these to be used by unauthorised persons. Particular care should be taken with group emails where the privacy of recipients needs to be protected. If there is any risk of the privacy of recipients being compromised, the BCC for individual addresses must be used.

8.2. Data Breach

Any GGS employee who either has knowledge of or loses, miscommunicates or has any data infiltrated by an external source must report it to the GGS Risk Manager as soon as possible. The GGS Risk Manager will provide advice in consultation with members of the GGS Data Breach Committee.

9 Breach

9.1. Should a person breach the terms of this Policy, the School may at its sole discretion respond to that breach having regard to matters considered relevant by the School.

9.2. To avoid doubt, an Authorised User who encourages, participates or otherwise knowingly acquiesces in conduct of another person which breaches the terms of this Policy, may also be found to have engaged in prohibited use in breach of the terms of this Policy.

9.3. In investigating a suspected breach of this Policy, the School may:

- Audit and inspect the ICT equipment/devices used in the alleged incident, including privately owned or leased ICT equipment; and
- Take all reasonable measures to preserve any related evidence, including copying of any data and/or seizing any ICT equipment/devices used in the alleged incident.

9.4. The Authorised User agrees to make promptly available the ICT equipment/devices available to the School for the purpose of any investigation and/or audit and to otherwise co-operate with the School in any investigation and/or audit process.

9.5. While the terms of this Policy do not form part of the terms and conditions of employment of staff members by the School, a breach of this Policy may result in disciplinary action including termination of employment.

9.6. The School may at its sole discretion take disciplinary action as appropriate against an Authorised User found to have breached the terms of this Policy, such disciplinary action may include, but is not limited to:

- Withdrawal of the Authorised User's authority to access and use School ICT and School ICT equipment/devices;
- Confiscation of any School ICT equipment/devices in the possession of the person; and/or
- Suspension or termination of employment.

9.7. A breach of the terms of this Policy may amount to a contravention of State and/or Federal legislation, and may constitute criminal misconduct. In such situations the School reserves the right to involve law enforcement agencies in addition to any disciplinary action it may take.

10 Queries or concerns

10.1. Queries or concerns must be taken to the Head of Campus. In the event of a serious incident which occurs when the Head of Campus is not available, a member of the School senior management must be notified immediately.

11 Liability of the School

11.1. The School makes no warranties of any kind, whether express or implied, in relation to use of School ICT and/or privately-owned or leased ICT on the School site or at any School-related Activity.

11.2. The Authorised User agrees use of any information obtained via use of School ICT and/or privately-owned or leased ICT on the School site or at any School-related Activity, in particular the Internet, is at his or her own risk and the School will not be responsible for any loss or damage, including consequential loss or damage, arising from use of School ICT by the Authorised User.

11.3. The Authorised User agrees to fully indemnify the School in respect of any loss and damage (including consequential loss or damage) arising from the Authorised User's use of School ICT and/or privately-owned or leased ICT on the School site or at any School-related Activity and/or any breach by the Authorised User of the terms of this Policy, and from and against any claim or proceeding (including costs of that claim or proceeding) that may be brought by any person against the School as a consequence of the Authorised User's use of School ICT and/or privately-owned or leased ICT on the School site or at any School-related Activity and/or any breach by the Authorised User of the terms of this Policy. The indemnity provided by the Authorised User to the School pursuant to this clause will apply notwithstanding any act or omission (whether negligent or otherwise) of the School or its agents.

12 Severability

12.1. If a Court determines that a word, phrase, sentence, paragraph or clause of this Policy is unenforceable, illegal or void then it shall be severed and the other provisions of this Policy shall remain effective.

13 Governing Law

13.1. The law of this Policy is the law of Victoria and the Commonwealth of Australia.

13.2. The parties submit themselves to the exclusive jurisdiction of the Courts of Victoria and the Commonwealth of Australia for all proceedings arising in connection with this Policy which proceedings shall be issued in Victoria.

14 Interpretation

14.1. The parties agree the introduction, definitions and rules and explanations sections, headings and acknowledgement page to this Policy also form part of its operative part.

Rebecca Cody
Principal

June 2018