

# Information Technology Policy

---

## 1. Statement of Commitment to Child Safety

The Geelong College is a Child Safe School. We have a zero-tolerance stance on child abuse and are committed to the protection of all children from all forms of abuse. The Geelong College recognises that in order to achieve a child safe environment at the College which meets students' intellectual, physical, social, emotional and moral needs, students need to be involved in the creation and maintenance of such an environment.

We are committed to taking a preventative and proactive approach to providing a child safe environment where children and young people are safe and feel safe; they are empowered to use their voices when decisions are being made that affect their safety. We are also committed to providing simple and accessible processes to assist all children to identify and communicate when they do not feel safe. Particularly, this includes those who are Aboriginal and Torres Strait Islander, from culturally diverse backgrounds and those with a disability.

We are clear about our behavioural expectations of every person in our community and are committed to having a shared understanding of and responsibility for child safety. All staff are expected to uphold a culture that protects children from all forms of harm.

## 2. Purpose

The purpose of this policy is to set appropriate acceptable use parameters for the Information Technology systems, to ensure the appropriate, effective and equitable use of The Geelong College's ICT network.

## 3. Scope

This policy sets out the Information and Communication Technology (ICT) resource rules that apply to all Staff, including Council Members of The Geelong College.

## 4. Access

The Geelong College provides Information and Communication Technology (ICT), including hardware, software, email, the internet, for use as a tool for educational use and to support College activities.

Use of these resources is encouraged and it is expected that:

- a) activities do not hinder or infringes on the rights or privacy of others
- b) the security of the College's ICT resources is maintained
- c) the reputation and/or integrity of the College and its staff are maintained at all times
- d) internet resources, such as email, social networking sites, and the internet are used appropriately and lawfully
- e) copyright and intellectual property are respected
- f) a Duty of Care for students and staff is complied with at all times

## 5. Security

In using College's ICT network staff are:

- a) presumed to be responsible for all activities undertaken using their accounts
- b) to protect the security of data held on mobile systems (eg phones, laptops, memory sticks and other storage mediums)

- c) not to connect unauthorised devices to the network, either via software or hardware that makes this possible (eg attaching a personal computer or external storage device)
- d) to must make sure that important College data that is not included in automatic backups is manually backed up on a regular basis and can be recovered to the latest version in the event of data loss
- e) staff to keep their username and password secure and private
- f) To log off or lock a computer before they move away from it
- g) To secure equipment (including staff allocated laptops, loan equipment such as projectors, recording equipment, etc) must always be kept in a locked area, or in staff's possession
- h) issues with the ICT equipment, to be advised to the Information Technology Services (ITS) department immediately so the issue can be addressed
- i) Staff must not to attempt to circumvent or compromise network security
- j) to immediately inform the College in accordance with the Data Breach Response Policy or a security breach.

## **6. Privacy, Copyright, Ownership of data and intellectual property**

- a) Staff will have access to and use of the private information of other College staff, students and community members as required by their duties. This information can only be used for College purposes and should not be shared with others unless required or directed to do so
- b) Email is not necessarily secure or confidential. It may be compromised by the unintended redistribution of email. Staff are advised to exercise caution at all times when using email.
- c) When using any College ICT System, staff members are expected to follow copyright law in accordance with any licence agreements.
- d) Subject to the College's statutes and regulations, the College is the owner of all data:
  - i. created by employees as part of their employment; and
  - ii. created, sent or received by users using the systems; and
  - iii. all such data may be accessed as records of evidence, including in an investigation or in response to other actions such as audit, litigation or criminal investigations.

## **7. Online Behaviour**

- a) The College ICT network must not be used as a medium to bully, harass, threaten or intimidate other users. Staff behaviour online should reflect appropriate and acceptable behaviour offline or in person; treating others fairly and with common courtesy.
- b) Staff should not intentionally access, modify, copy or move other staff members' or students' personal files or settings, aligned to expectations of the Staff and Council Code of Conduct
- c) Staff must not install or store inappropriate, illegal or unlicensed software on College computers or on the network. However, the College recognises that staff may wish to put other applications on their allocated equipment. This is permitted so long as the applications:
  - i. Allow sufficient memory and hard drive space to keep computers operational
  - ii. Are currently licensed to the user
  - iii. Do not interfere with the configuration of computers
  - iv. Are not used inappropriately
  - v. Do not interfere with the operation of the College network
- d) Staff should not allow other users direct access to their computer through file sharing.
- e) Any personal use of College equipment and systems should be incidental and not interfere with the users role within the College, the work or study of others or the operation of the systems.

## **8. Internet Usage**

Staff are expected to comply with the following:

- a) Internet access at the College is provided for educational use and therefore personal use should be limited. The College's internet connection is filtered to prevent access to sites which are deemed inappropriate for college use.
- b) Be conscious of the quantity of data consumed when accessing the internet (including for educational purposes) and avoid unnecessary or excessive use.
- c) Staff exercise care when using the internet and should not seek to access or download inappropriate, offensive, discriminatory or intimidating material.
- d) Intentionally accessing, storing or distributing material that is inappropriate, offensive, discriminatory or intimidating in nature, or which puts any member of the community at risk may lead to disciplinary action. This may involve reporting the matter to police where State or Federal laws have been breached.
- e) When obtaining information from the Internet, staff are not to infringe the copyright of others by using the information without permission or acknowledgement of the copyright holder.
- f) Staff are to exercise caution when downloading files from the internet, as these may contain viruses, adware or spyware. Anti-virus software is provided on all College-supplied computers, and staff should scan their computer regularly to ensure that it is free from infections.
- g) The College restricts access to some material available via the internet, but does not accept responsibility for any illegal, offensive, indecent or otherwise harmful material accessed on the Internet, nor for any loss arising from use of, or reliance on, information obtained through its Internet service, or in relation to the reliability or quality of that service. Staff are not permitted to bypass filtering software to enter any site which contains material of an illegal, offensive or otherwise harmful nature. The College will not be responsible for any loss or liability incurred by staff through their use of the internet.

## **9. Email Usage**

- a) Email carries the same legal status as a signed letter or memo. It is considered a formal means of communication, and care should be taken when composing and sending email. Responsible use of the email system is based on common sense, common decency and civility, and should not be used when face-to-face communication would be more appropriate.
- b) Staff are not to send unsolicited email to multiple recipients and distribution of email should be limited to necessary recipients only; the need to send global ('All Staff') emails should be carefully considered.
- c) Staff must not distribute or forward 'spam', hoax or 'chain' emails.
- d) College disclaimers will automatically appear on all external email communications

## **10. Printing**

- a) Care and conservation should be paramount considerations with regard to the use of College printing facilities. Staff minimise printing and consider the environment when using print facilities.
- b) Staff should review documents on screen, and students should submit work electronically where appropriate.

## **11. School Sanctioned Platforms**

The College has defined software platforms, data storage facilities, and other such ICT resources to enable staff to carry out their duties. It is not acceptable for a staff member to use a platform

to perform their duties that is not prescribed by the College. For example, a teacher must not use software to manage student learning that is outside that which is resourced by the College.

If a teacher wishes to use software relevant to their subject area and it has not been endorsed by the College, they must seek approval from their campus Head of Learning and Curriculum at first instance.

## **12. Monitoring**

The College reserves the right to, at any time, and without prior notice, examine email messages, files stored on computers and in network locations, internet favourites, history and cache files, and other information stored on computers and on the network, for material or activity that would constitute a breach of this policy. As well as pass on the information to external organisations where legally obliged to do so.

## **13. Infringements**

If a staff member is found engaging in activity contrary to this policy, their computer access privileges may be suspended and disciplinary action may be taken. If a staff member is suspected of engaging in activity contrary to law, his/her access privileges will be suspended and he/she may be liable to prosecution.

## **14. Related Documents**

[Rules on Staff use of Social Media](#)

[Internet Filtering Policy](#)

[Staff Code of Conduct](#)

[Privacy Policy](#)

[Staff Workplace Behaviour Policy & Procedure](#)

[Data Breach Response Plan](#)