

Network User Policy

1. Purpose

To document the policy for staff and student usage of The Gordon computer network and Information Systems.

2. Scope

This policy applies to all staff, students and contractors of The Gordon and is inclusive of all The Gordon campuses, including Fenwick Street, Boundary Road, Colac and Wyndham campuses.

This policy governs all computers, computing laboratories, libraries and open access areas across the Institute together with use of all associated networks, internet access, email, hardware, data storage, computer accounts, software (both proprietary and those developed by the Institute), telephony services and voicemail.

3. Policy

Use of The Gordon's computer network, email system and public Internet / Intranet by Gordon staff, students and contractors is permitted and encouraged where such use is suitable for educational purposes and supports the goals and objectives of The Gordon learning outcomes. The network is to be used in a manner that is consistent with The Gordon's standards of conduct and as part of the normal Institute educational environment.

3.1 General principles

The use of Gordon computer and Information Systems is consistent with other Gordon policies specifically relating to:

- *Copyright Act 1968*
- *Equal Opportunity Act 1995*
- *Freedom of Information Act 1982*
- *Privacy Act 1988*
- *Racial Discrimination Act 1975*
- *Sexual Discrimination Act 1984*

Provision of Gordon resources such as Internet / Intranet, email privileges, computer systems and networks for Gordon students, are intended to be used by:

- Students for educational purposes only and acceptable use is defined as:
 - Activities directly related to the day-to-day course and study requirements.
 - Research, discussions and associated activities related to current or future areas of study.
- Staff and contractors for business purposes only. Acceptable use is defined as:
 - Activities directly related to the day-to-day operations and business of the Institute.
 - Research, discussions and associated activities for professional development to directly support the operations of The Gordon.

Use of the Internet / Intranet and e-mail is subject to monitoring for security and/or network management reasons. The distribution of any information through the Internet, computer-based services, email and messaging systems is subject to the scrutiny of The Gordon. The Gordon reserves the right to determine the suitability of this information.

3.2 Access

Access to The Gordon computer network, email system and public Internet/Intranet by Gordon staff, students and contractors may only be gained by the use of an authorised network access account.

Persons other than Gordon staff, students and contractors may not be provided with network access by The Gordon unless such access has been approved by Corporate Information Solutions.

Gordon staff, students and contractors must not transfer accounts or make accounts available to a person other than the account holder. Responsibility and accountability for network security are the shared responsibility of all network users. It is your responsibility to protect your password and not divulge it to another person.

If you know or suspect that your account has been used by another person, you must notify the Corporate Information Solutions immediately.

3.3 Conditions of use

The following practices are considered unacceptable, and may be subject to disciplinary action, including warnings, revocation of access privileges, and, in extreme cases, termination of study.

The Gordon also reserves the right to report any illegal activities to the appropriate authorities:

- Visiting Internet sites that contain obscene, hateful or otherwise objectionable materials; storing, sending or receiving any material that is obscene or defamatory, or that is intended to annoy, harass or intimidate another person¹.
- Students must not use The Gordon network to harass, abuse or otherwise seek to offend or discriminate against others, refer to *Student Misconduct Management Procedure QA PR 11 and Prevention of Bullying in the Workplace SHRD PO 27*.
- Sending or receiving unusually large emails or attachments; sending or forwarding electronic chain letters.
- Due to the shared nature of Institute storage, very large documents, video or high resolution images should not be accessed, transferred or stored on the network unless directly related to study purposes.

¹ Obscene or offensive material is defined as:

“Material that depicts matters of sex, drug misuse or addiction, crime, violence or revolting or abhorrent phenomena in a way that offends the standards of morality and decency generally accepted by reasonable adults.”

- Wasting time on non-educational pursuits.
- Soliciting emails that are unrelated to study activities, or using Gordon resources for personal gain or profit.
- Representing personal opinions as those of the Institute.
- Using the Internet or email for gambling or illegal activities.
- Making or posting indecent remarks, proposals or materials.
- Uploading, downloading or otherwise transmitting copyrighted material in violation of its copyright, refer to *Copyright Policy TED PO 06*
- Downloading any software or electronic files without implementing virus protection measures that have been approved by The Gordon.
- Intentionally interfering with normal operation of the network, including the propagation of computer viruses, or sustained high volume network traffic that substantially hinders others in their use of the network.
- Revealing or publicising confidential or proprietary information including, but not limited to: student information, financial information and commercially confidential information, refer *Privacy Policy RM PO 04 and Release of Student Information RM PR 06*.
- Examining, changing or using another person's files, output or user name without explicit authorisation.
- Other inappropriate uses of Internet/Intranet or network resources that may be identified by the network administrator.
- Unauthorised access to or modification of internal computer, computer peripheral or network devices. This includes the unauthorised connection of any device to The Gordon network, but excludes user-accessible components such as printer cartridges and paper trays.
- The unauthorised installation of any software onto Gordon computers.

3.4 Publishing

If you wish to publish information relating to and on behalf of The Gordon, you must obtain permission to do so from the Chief Executive Officer or his / her authorised delegate. The authorised source and author of official Gordon information must be identified in published material of that nature.

All Gordon logos and designs are the property of The Gordon and may only be used for Gordon documents approved by the Chief Executive Officer or his / her authorised delegate.

3.5 Further information

For clarification on any matter in relation to this Code of Practice, please contact the ICT Enterprise Systems Infrastructure Manager, or e-mail cisservicedesk@gordontafe.edu.au.

4. Procedure

There is no Procedure pursuant to this Policy.

5. Responsibilities

Position	Responsibility / Governance
The Manager ICT Enterprise Systems Infrastructure	For the implementation and maintenance of this Policy.
Head of People, Safety and Culture and Operations and Employee Experience	For ensuring that all new staff have completed a Network User Application prior to new user account activation.
Gordon Staff and students	To abide by The Gordon computer network and Corporate Information Solutions access and conditions of use requirements as documented in this policy.

6. Definitions

There are no definitions arising under this Policy.

7. Key aligned internal documents

Refer to the [Operational Management System \(OMS\)](#) for copies of all policies, procedures and supporting documents.

Network Usage Account Authorisation IS FO 03.01

Student Misconduct Management Procedure QA PR 11

Privacy Policy RM PO 04

Release of Student Information RM PR 06

Equal Opportunity Policy SHRD PO 15

Prevention of Bullying in the Workplace SHRD PO 27

Copyright Policy TED PO 06

8. Key Aligned Legislation / Documents

[Copyright Act 1968](#)

[Equal Opportunity Act 1995](#)

[Freedom of Information Act 1982](#)

[Privacy Act 1988](#)

[Racial Discrimination Act 1975](#)

[Sexual Discrimination Act 1984](#)

9. Review and Approval

Business Process Owner	Chief Information Officer, Corporate Information Solutions		
Endorsed by (if applicable)	Not applicable	Endorsed Date	
Approved by (if applicable)	Not applicable	Approved Date	26 October 2023
Review schedule	This policy will be reviewed every 3 years (or earlier as required)		
Date of next review	26 October 2023		