POLICY TITLE: Acceptable Use of IT and Communication Systems

Purpose

The purpose of this policy is to outline the Photography Studies College (Melbourne) policy on the use of the College's IT and Communication Systems, including but not limited to the College's Internet, Intranet, ICT systems and College provided email accounts.

This policy also explains the consequences for individuals that use the College's IT and Communication Systems for unauthorised purposes.

Policy

Use of the College's IT and Communication Systems by employees, contractors, Committee Members, students and graduates is permitted and encouraged where such use is suitable for business and educational purposes and supports the goals and objectives of the College. In particular, the IT and Communication Systems are to be used in a manner that is consistent with acceptable standards of behaviour, codes of conduct and as part of the normal execution of student studies, graduate alumni activities and work responsibilities.

Photography Studies College (Melbourne) IT and Communication Systems should not be used for anything other than College sanctioned communications.

The use of the College's IT and Communication Systems is subject to Australian law and any illegal use will be dealt with appropriately.

Note that electronic devices supplied by the College (e.g. mobile phones, tablets) come with limited data allowances for both email and Internet access for work related activities.

Unacceptable use

When using the College's IT and Communications Systems, users shall not:

- Visit Internet sites that contain obscene, hateful or other objectionable materials.
- Make or post indecent remarks, proposals or materials on the Internet.
- Publish defamatory and/or knowingly false material about the College, students, colleagues and/or our clients on any form of social media (which includes, but is not limited to social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format).
- Solicit emails that are unrelated to business activities or for personal gain.
- Send or receive any material that is obscene or defamatory or which is intended to bully, harass, discriminate or intimidate another person.
- Represent personal opinions as those of the College.

- Use any other email accounts and/or software except that which is sanctioned by the College.
- Distribute Trojan horses, worms, malicious or destructive code or any instructions activating such code.
- Engage in “time-wasting” activities unrelated to the business of the College

Users must observe the confidentiality of information managed by the College and shall not:

- Upload, download or otherwise transmit information in a manner that infringes any other person’s (including the College’s) intellectual property rights, without the consent of the owner.
- Reveal or publicize confidential or proprietary information which includes, but is not limited to: financial information, new business and product ideas, marketing strategies and plans, databases and the information contained therein, customer lists, technical product information, computer software source codes, computer/network access codes, passwords and business relationships.

Security

Maintaining proper security over the organisation’s ICT systems is critical. The College as part of its approach to security maintains:

1. Internal checklist in regulation with Small Business Cyber Security
2. 360 South Website Maintenance Plan
3. The College holds a Cyber Event Protection Policy via Emergence

Users shall not:

- Download any software or electronic files without first gaining the direct permission of an authorised manager in consultation with ICT technicians and then implementing virus protection measures that have been approved by ICT technicians.
- Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network.
- Examine, change or use another person's files, output or username for which they do not have explicit authorization.
- Perform any other inappropriate uses identified by the Network Administrators

This policy also applies to cellular telephones and personal digital assistants (PDAs) – such as smartphones and other electronic tablets. These devices enable fast communications, remote wireless network connectivity and more productive mobile employees. However, such devices add significant additional security concerns for the organisation.

All devices which have been provided by the College, or which have access to the College’s IT and Communication Systems must have automatic keypad locking and pin codes to restrict access to the authorised user. Applications loaded to these devices are subject to this policy.

Monitoring

Uses of Internet/Intranet and email may be subject to monitoring for security and/or network management reasons. Users may also be subject to limitations on their use of such resources.

The distribution of any information through the Internet, computer-based services, email and messaging systems are subject to periodic inspection. Photography Studies College (Melbourne) reserves the right to determine the suitability of information distributed.

Obligation to report breaches of the policy

If you believe this policy has been breached and wish to make a complaint please bring the matter to the attention of the Chief Information Officer or in their absence, the Managing Director.

Responsibility

Management
All employees
Students
Graduates granted access to the College's ICT
Any individual who uses the College's IT or Communication Systems

Definitions

Nil

Related Documentation

Policies

Staff Code of Conduct
Student Code of Conduct
Social Media

Procedures Forms & Documents

Staff Handbook
I.T Matrix: Software Provider Responsibility Guide
Cyber Event Protection Policy via Emergence (Policy No. CS 22059410A/00/01)

Publishing Details

Policy number: HR012_v5_HED_VET	**Status:** Final
Approved: 30/06/2022	**Review Date:** June 2025
Julie Moss - Managing Director	**Published:** July 2022