ACCEPTABLE USE OF IT RESOURCES

Section 1 - Purpose and Scope

(1) The purpose of this Policy is to specify the requirements for the respectful, safe, reliable and secure use of IT Resources provided by the College.

Note: This includes, but is not limited to, Internet usage and email activity.

Scope

(2) This Policy applies to:

(a) all technology resources used by, operated by, or provided on behalf of the College;

(b) all information collected, created, stored or processed by, or for the College on computer or network resources; and

(c) all individuals who use, or are involved in deploying and supporting, computer and network resources provided by the College. This includes, but is not limited to, all staff, all students, contractors, volunteers and visitors (also referred to as "users").

Section 2 - Definitions

(3) In this Policy:

(a) **Authorised purposes** means:

i. Activities associated with work or study at the College; and / or

ii. The provision of services to or by the College, which are approved or authorised by the relevant officer or employee of the College in accordance with College policies, procedures or contractual obligations, including limited personal use, or any other purpose authorised by the relevant officer or employee.

(b) **Hacking tools** means tools that are designed to facilitate the identification and exploitation of software or system weaknesses (including but not limited to sniffing, scanning or password guessing) for the purposes of unauthorised access.

(c) **Information Technology** or **IT Resources** includes, but is not limited to:

i. All computers and all associated data networks and systems, internet access and network bandwidth, email, hardware, data storage, computer accounts, media, software (both proprietary and those developed by the College) and telephony services.

ii. Information Technology services provided jointly, or as part of a joint venture with another organisation affiliated or partnering with the College.

iii. Information Technology services provided by third parties that have been engaged by the College.

iv. Security controls or protection mechanisms means systems or facilities implemented by individuals who are authorised by the College to access or utilise the resource or information.

Section 3 - Policy Statement

Acceptable use

(4) All individuals who access, use or otherwise engage with the College's IT Resources must:
- (a) respect the rights of all individuals, including other users;
- (b) only use or modify the College's IT Resources for **authorised purposes**, and not in breach of relevant laws or contractual obligations;
- (c) not use College computer or network equipment for non-commercial personal purposes beyond a reasonable amount, or to the detriment of the College or its goals;
- (d) not access, distribute, store or display illegal, pirated or offensive material;
- (e) not use College computer or network equipment for unauthorised personal financial or commercial gain;
- (f) not misrepresent the views of the College, via use of the College's IT Resources;
- (g) not conduct activities that consume excessive network bandwidth;
- (h) report suspected or actual security breaches to their Manager, the IT Services Staff, or the CEO in a timely manner; and
- (i) maintain the security and confidentiality of information generated or collected by the College in accordance with the relevant requirements.

(5) Further examples of activities that are not permitted are set out at Schedule 1.

(6) The College considers any display or transmission of offensive or sexually explicit material to be unacceptable and will not be tolerated. The transmission of such material, even if sent from outside sources, is strictly forbidden and may lead to immediate termination of employment or engagement or disciplinary action taken.

Secure System Access and Use

(7) To protect access to the College's IT Resources, individuals are required to:
- (a) select long and strong passwords that are not easily guessed and not in use in other non-College applications;
- (b) not share College-provided or self-selected passwords with other individuals;
- (c) keep personal and College-provided systems, used to access College systems or information, free from known vulnerabilities by keeping up-to-date with vendor provided security updates;
- (d) maintain operational and up-to-date antivirus protections on personal and College-provided systems used to access College systems or information;
- (e) securely store passwords that provide access to College systems or information;
- (f) only use the accounts provided by the College for their own individual use;

(g) not bypass or attempt to circumvent the College's security controls or protections;
(h) not introduce malicious software such as viruses, worms, ransomware or trojans into the College environment; and
(i) not use **hacking tools** when accessing, using or otherwise engaging with College IT Resources.

Monitoring and Compliance

(8) The College reserves the right to monitor its IT Resources and information systems for compliance with this and other College policies. It may, at any time:
(a) undertake a monitoring activity of all or part of its IT Resources; and
(b) remove illegal or inappropriate material.

(9) Examples of the types of monitoring and other controls that may be undertaken include:
(a) random audits;
(b) requiring appropriate approvals (including delegation of authority);
(c) disclosing usage;
(d) maintaining accurate records;
(e) monitoring records; and
(f) access control (such as network firewalls and web filtering tools).

Note: Monitoring by the College may take place on a continuous and ongoing basis. Employees should therefore assume that all email correspondence may be opened by College management.

(10) Breaches of this Policy constitutes misuse of College information and information systems.
(a) If misuse of IT Resources is detected or suspected, relevant disciplinary processes will apply.
(b) Serious matters may result in civil and / or criminal proceedings.

(11) The College has a statutory obligation to report illegal activities and corrupt conduct and will cooperate fully with the relevant authorities.

(12) To the extent allowed by law, the College is not liable for loss, damage or consequential loss or damage arising from the use of misuse of any IT Resources.

(13) Monitoring information (refer clauses 8 and 9) may be subject to viewing by or disclosure to:
(a) the IT Services team;
(b) a senior manager where there is reasonable suspicion of contravention of this Policy and a request to review use has been approved by the CEO;
(c) the CEO; and / or
(d) when required by law, for example on receipt of a subpoena.

(14) In addition, the content of emails may be accessed:

(a) where there is reasonable suspicion of contravention of this Policy and a request to access the contents of a user's email has been approved by the CEO, or
(c) where required by law, for example on receipt of a subpoena.

Restricting or Blocking Access

(15) The College may, at any time and without notifying Users, restrict or block access to various internet sites and applications.

> Note: Certain file types, such as multimedia files (e.g. mp3, mpg, avi), may be automatically blocked by IT Services.

(16) Any use of programs to subvert or attempt to subvert the College's filters in order to access blocked internet sites and/or applications will amount to a breach of this Policy.

SCHEDULE 1: EXAMPLES

(17) The following is a list of further examples of activities that are not permitted using IT Resources, unless specifically authorised by the appropriate officer.

(a) Intentionally accessing, creating, transmitting, distributing, or storing any offensive information, data or material that violates Australian or State regulations or laws.
(b) Using IT Resources for non-ACPE business or commercial purposes.
(c) Promoting any advertising or sponsorship except where such advertising or sponsorship is clearly related to ACPE business and has the approval of the CEO.
(d) A user representing themselves anonymously or as someone else, whether real or fictional, when sending email or posting information (for example, on the Internet).
(e) Using another user's ACPE email account to send email messages unless given explicit permission to do so through the use of Outlook permissions.
(f) Using another individual's account to access the Internet.
(g) Undertaking any form of computer hacking (illegally accessing other computers).
(h) Intentionally sending or forwarding chain letters.
(i) Users using their ACPE email address for the purpose of subscribing to mailing lists except in relation to work, study or professional development purposes.
(j) Users using their ACPE email address to subscribe to social networking sites where the email address is displayed to other users, unless the CEO has provided approval for the user to subscribe to the site in their work capacity.
(k) Using IT Resources for activities that may be questionable, controversial or offensive, such as gambling, gaming, accessing chat lines, transmitting inappropriate jokes or sending junk programs.
(l) Using Internet services for Internet Relay Chat ("IRC") and File Transfer Protocol ("FTP") services at any time without approval from the CEO.

(m) Transmitting any non-business related written material to political organisations.
(n) For staff - Automatically forward email messages to an external email account without approval from the CEO.
(o) Intentionally transmitting externally, copyrighted material or material over which subsisting intellectual property rights exist (including ACPE teaching material) without the express permission of the owner.
(p) Transmitting an advertisement of goods or services available for sale or hire
(q) Intentionally undertaking any activity intending to have a detrimental effect on storage, processing or communications network services (i.e. viruses, chain letters etc.)
(r) Using private email accounts as an alternative to their ACPE email account for sending or receiving any ACPE official communication relating to ACPE business activities.
(s) For staff - Use any online third-party storage service (e.g. cloud storage facilities such as Google Docs, Google Drive and Dropbox) for the permanent or temporary storage of any Legal APCE official information unless approved by the CEO.
(t) Transmitting any ACPE official material to media organisations without the explicit approval of the CEO.
(u) Streaming, or downloading from and uploading to the Internet, of video and music files is prohibited at any time unless directly related to a staff member's employment at the College and provided there is no unauthorised use of copyright material.
(v) unauthorised recording, publishing, or communication of lectures, tutorials, meetings or conversations.
(w) Download program files (i.e. executable software), including free trials. Staff members seeking access to additional software must seek formal approval from IT Services.

Section 4 - Procedures

(18) Nil.

Section 5 – Guidelines

(19) These guidelines relate to the protocols that staff members, in particular, should follow in respect of the ACPE emails (that is, the emails provided by ACPE Ltd for use by staff and students (*@acpe.edu.au) and includes attachments.

(a) Email is a business communication and sending it is classed as a business transaction. Sending an email message from an ACPE email account is similar to sending a letter on ACPE letterhead.

(b) Depending on its content, an email message may constitute a formal business record. If this is the case, the user who sends or receives the message must

ensure the message is stored in an appropriate place (e.g. electronic or hard copy file).

(c) Email does not have a guarantee of security. Where possible, highly sensitive or confidential documents should not be sent via email. If in doubt, a User must check with their manager.

(d) Users should:
  (i) ensure that the form and content of work-related emails are drafted in a professional and appropriate manner;
  (ii) only distribute messages to relevant parties (as addresses or copied-in); and
  (iii) write emails in sentence case rather than capitals (which can appear threatening and unfriendly).

Related documents

This Policy should be read in conjunction with but not limited to:

a. Social Media Policy
b. Social Media Procedure
c. Staff and Student Codes of Conduct
d. Workplace Surveillance Policy

Document Administration

Policy Name	Acceptable Use of IT Resources
Policy Owner	CEO
Approval Authority	Board of Directors
Approval Date	17 April 2023
Effective Date	As at Approval Date
Next Review #	Three years from the Approval Date
Amendment history	
Version 1:	Document developed and implemented. This document replaces the Internet and Email Policy (POL-51).

 # Unless otherwise indicated, this Policy will still apply beyond the Review date