ACPE
AUSTRALIAN COLLEGE OF PHYSICAL EDUCATION

POLICY DOCUMENT

INTERNET AND EMAIL POLICY

1. Purpose and Scope

Purpose

1.1 ACPE (The College) recognises that its computer, email and internet resources are critical tools of the College workplace, however there are a number of serious risks or consequences that may affect the College, its employees or customers if these resources are misused.

1.2 This policy sets out the appropriate standard of behaviour for users of the College's computer, email and internet resources and should be read in line with the College's Workplace Surveillance and Social Media Policies.

Scope

This policy applies to all users who access or use the College's computer, email and internet resources, including but not limited to employees, contractors, consultants, volunteers and those performing work experience ("Users").

2. Policy

2.1 Policy Principles

This policy recognizes internet and email services are provided by ACPE Ltd for business use.

2.1.1 All staff have a responsibility to be ethical and efficient in their official or private use of College property and services.

2.1.2 All staff have a responsibility to be productive in the use of their work time.

2.1.3 Staff are increasingly being encouraged to engage online as part of their work.

2.1.4 Staff are also private citizens with individual personal needs and obligations.

2.1.5 Staff may need to make use of the Internet and email for personal purposes.

2.1.6 There is a reasonable limit to which employer provided Internet and email services may be used for personal purposes.

2.1.7 Staff should be provided with guidelines that clearly outline their rights and responsibilities on the use of Internet and email and that there will be consequences for any inappropriate use and/or contravention of this policy.

2.2 Responsibilities

In providing staff with access to Internet and email services, ACPE will:

i. Provide staff with a clear statement of their responsibilities when using the Internet and email
ii. Ensure an automated disclaimer is included on all messages sent to external recipients making it clear that the opinions expressed are those of the sender and not ACPE
iii. Notify staff that ACPE will monitor Internet usage and email activity

2.2.1 Chief Executive Officer / Dean

The CEO/Dean has the responsibility of engendering a commitment to the values espoused by this policy and ensuring adequate controls are in place to administer the policy. Controls may include systems for:

i. Random audits
ii. Appropriate approvals (including delegation of authority)
iii. Disclosure of usage
iv. Maintaining accurate records
v. Monitoring records, and
vi. Access control (e.g. network firewalls and web filtering tools)

All controls are subject to any relevant privacy legislation and/or guidelines.

If genuine business reasons require staff to access Internet sites that would be normally regarded as inappropriate, the CEO/Dean has a responsibility to ensure such access is undertaken in a suitably secure environment.

2.2.2 Managers

Managers and supervisors are responsible for:

i. Ensuring that staff are aware of and understand the policy
ii. Monitoring, and where necessary, enforcing policies, and
iii. Providing leadership by example

2.2.3 Information Technology Services Team (or delegate)

The Information Technology Services Team or delegate is responsible for:

i. Establishing appropriate security measures
ii. Controlling and monitoring access to email and the Internet
iii. Undertaking usage audits on a regular basis
iv. Promote awareness and understanding of this policy

2.2.4 Staff

All staff are personally accountable in their use of work resources and share a responsibility for ensuring that:

i. Official resources are used ethically
ii. They apply due economy and efficiency in use
iii. Steps are taken to protect confidentiality that are appropriate to both the information involved and the service being used
iv. They adhere to the requirements of this policy and any associated guidelines or procedures, and
v. They report breaches of this policy to their manager.

2.3 Use of Computer, Email and Internet Resources

2.3.1 Users are entitled to access and use the College's computer, email and internet resources for business purposes.

2.3.2 Limited private use of the College's computer, email and internet resources is permitted subject to the following conditions:

i. private use must be kept to a minimum;
ii. private use must not interfere with or delay a User's work obligations in any way; and
iii. private use must comply with all College policies and must not be inconsistent with the User's contract of employment or contractor agreement.

2.4 Material

2.4.1 The display or transmission of offensive or sexually explicit material is unacceptable and will not be tolerated. The transmission of any such material by Users, even if sent from outside sources, is strictly forbidden and may lead to immediate termination of employment or engagement.

2.4.2 All computers and the data stored on them are and remain at all times, the property of the College. As such, all email messages composed, sent, and/or received are the property of the College.

2.5 Inappropriate Use

2.5.1 The use of the Internet or email to make or send fraudulent, unlawful, offensive or abusive information or messages is prohibited. Staff are to report receipt of any such messages to their immediate manager. Any staff member identified as the initiator of such information or messages is subject to disciplinary action and possible criminal prosecution.

2.5.2 Examples of inappropriate use of College computer, email and internet resources include (but are not limited to):

i. use for unlawful activities (e.g. hacking or intellectual property piracy);
ii. could damage the reputation of ACPE Ltd
iii. Could result in victimisation or harassment
iv. Could lead to criminal penalty
v. Could expose ACPE to civil liability

vi. Facilitates unauthorised access, modification or impairment of data on a computer

vii. use for activities that create an actual or potential conflict with the user's obligations to the College (e.g. sending sensitive information to a competitor);

viii. use of abusive language or graphics in either public or private messages;

ix. activities which could cause congestion and/or disruption of networks or systems (e.g. downloading large media files); and

x. accessing, viewing, posting, downloading, storing, transmitting, sharing, printing, distributing or soliciting of any information or material that the College views as racist, pornographic, obscene, abusive or otherwise offensive.

2.5.3 Staff may be individually liable if they aid and abet others who discriminate against, vilify or harass colleagues or any member of the public. Where inappropriate use is identified, ACPE Ltd has a responsibility to:

i. Consider implementing disciplinary action

ii. Notify the Police if it is reasonably believed a criminal offence has been committed.

2.5.4 Email messages must not contain material that is or could reasonably be considered offensive, defamatory, discriminatory or derogatory. Such inappropriate content would include, but is not limited to:

i. sexual comments or images;

ii. solicitation of non-business causes (including but not limited to political, religious causes unless the activity is a College sponsored or sanctioned activity);

iii. chain-letters;

iv. gender-specific comments, or any comments that might offend someone on account of his or her age, gender, sexual orientation, religious or political beliefs, national origin or disability; and

v. messages which have the potential to be viewed as defamatory, threatening or obscene.

2.5.5 Restricted Activities

In addition to the above, the following activities are not permitted using Internet and email services provided by ACPE Ltd. Staff must not:

i. Intentionally access, create, transmit, distribute, or store any offensive information, data or material that violates Australian or State regulations or laws.
ii. ACPE Ltd reserves the right to audit and remove any illegal material from its computers without notice.
iii. Use Internet or email services for non-ACPE business purposes.
iv. Promote any advertising or sponsorship except where such advertising or sponsorship is clearly related to ACPE business and has the approval of the CEO/Dean
v. Transmit information that is commercial in nature
vi. Represent themselves anonymously or as someone else, whether real or fictional, when sending email or posting information to the Internet.
vii. Use another staff member's email account to send email messages unless given explicit permission to do so through the use of Outlook permissions.
viii. Use another staff member's account to access the Internet.
ix. Undertake any form of computer hacking (illegally accessing other computers).
x. Intentionally send or forward chain letters.
xi. Use their ACPE email address for the purpose of subscribing to mailing lists except in relation to work or professional development purposes.
xii. Use their ACPE email address to subscribe to social networking sites where the email address is displayed to other users, unless the CEO/Dean has provided approval to use the site in their work capacity.
xiii. Use the Internet or email for activities that might be questionable, controversial or offensive, such as gambling, gaming, accessing chat lines, transmitting inappropriate jokes or sending junk programs.

xiv. Use Internet services for Internet Relay Chat ("IRC") and File Transfer Protocol ("FTP") services at any time without approval from the CEO/Dean.

xv. Use Internet and email services for the transmission of any non-business related written material to political organisations.

xvi. Automatically forward email messages to an external email account without approval from the CEO/Dean.

xvii. Intentionally transmit copyrighted material or material over which subsisting intellectual property rights exist without the express permission of the owner

xviii. Transmit an advertisement of goods or services available for sale or hire

xix. Intentionally, undertake any activity intending to have a detrimental effect on storage, processing or communications network services (i.e. viruses, chain letters etc.)

xx. Use private email accounts as an alternative to their ACPE email account for sending or receiving any ACPE official communication relating to ACPE business activities.

xxi. 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 and Dean.

xxii. Use Internet or email services to transmit any ACPE official material to media organisations unless in accordance with the ACPE Media Policy

2.6 Security

Email does not possess 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 his or her manager.

2.7 Monitoring Activities

2.7.1 The College reserves the right to monitor (log) email and internet use in order to maintain the standards set out in this policy and the security of our computer system. Senior managers of the College have the right to access information so logged.

2.7.2 System administrators and senior management have access to individual audit trails of email and internet use for necessary maintenance of the computer system. The College has the ability to monitor the use and operation of the College computer resources by means of software designed to filter the use of internet and email content and to monitor compliance with the College's policies. The College may conduct forensic computer examinations randomly and in the event of a suspected breach of policy.

2.7.3 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.

2.8 Restricting or Blocking Access

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

2.8.2 Any use of programs by Users to in any way subvert the College's filters in order to access blocked internet sites and/or applications will amount to a breach of this Policy.

2.9 Protocols

2.9.1 Users must ensure that the form and content of work-related emails are drafted in a professional and appropriate manner.

2.9.2 Similarly, consideration should be given to the distribution of a message and only relevant parties should be included as the addressees or be copied-in.

2.9.3 Emails should be written in sentence case rather than capitals. Capital letters appear threatening and unfriendly and tend to create an adverse impression.

2.10 Formal Business Records

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

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).

2.11 File Streaming, Downloading and Uploading

The streaming of or downloading from and uploading to the Internet of video and music files is prohibited at any time unless work related. Care needs to be taken to prevent unauthorised use of copyright material. Certain file types, such as multimedia files (e.g. mp3, mpg, avi), may be automatically blocked by IT Services.

Program files (i.e. executable software) are not to be downloaded under any circumstances. Employees requiring access to additional software must complete the appropriate form and forward it to the Service Desk. This process must be followed regardless of the licence type of the software (e.g. free trial, freeware etc.).

2.12 Disclosure

Monitoring information may be subject to viewing by or disclosure to:

2.12.1 The IT Services team on a regular basis.

2.12.2 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.

2.12.3 The CEO and Dean

2.12.4 Others where required to by law, for example on receipt of a subpoena.The Network Administrator IT Services or Network Officer IT Services in satisfying any of the above requests.

2.12.5 In addition, the content of emails may be accessed:

2.12.6 Where there is reasonable suspicion of contravention of this policy and a request to access the contents of email for a staff member has been approved by the CEO.

2.12.7 Where a request to access an email account is received from a supervisor/manager and complies with the requirements of the Procedure for Accessing Staff email Accounts.

2.12.8 To others where required to by law, for example on receipt of a subpoena.

2.13 Breach of this Policy

2.13.1 Any User who is found to have breached this policy may be subject to disciplinary action, up to and including termination of employment or engagement.

3. Definitions

3.1 email

Electronic mail service provided by ACPE Ltd for the use of staff in the form of an email account and ACPE email address (*@acpe.edu.au). Includes any and all messages sent using this email account including attachments.

3.2 Internet

All references to the Internet in this policy should be taken to include all online services including the World Wide Web (www), email, newsgroups, chat groups, message boards, social media services and file transfer protocol (ftp).

3.3 Staff

Any contract, permanent or temporary staff or consultant employed by ACPE Ltd

3.4 Work

This policy applies to staff when they are at a workplace of ACPE Ltd whether or not the staff member is actually performing work at the time, or at any other place while performing work for ACPE Ltd.

4. Related Documents

College policies and procedures:

- Staff Grievance and Appeals Policy

Legislation:

- Workplace Surveillance Act 2005
- Anti Discrimination Act 1977
- Privacy and Personal Information Act, 2002

5. Document Administration

Policy Name & Code:			Internet and Email Policy (POL-51)
Policy Owner:			HR/ CEO and Dean
Approval Authority:			Board of Directors
Next Review:			September 2023
Approval Date	**Effective Date**	**Version**	**Summary of changes**
09.04.20	10.04.20	1	Approved by Board of Directors.

* Unless otherwise indicated, this policy will still apply beyond the review date.