



Information Technology Usage Policy and Procedure

CONTENTS

| | | |
|---|--|---|
| 1 | PURPOSE..... | 1 |
| 2 | SCOPE..... | 1 |
| 3 | POLICY STATEMENT | 1 |
| 4 | PROCEDURES..... | 1 |
| 5 | RESPONSIBILITIES | 3 |
| 6 | DEFINITIONS | 4 |
| 7 | RELATED LEGISLATION AND DOCUMENTS..... | 4 |
| 8 | FEEDBACK..... | 4 |
| 9 | APPROVAL AND REVIEW DETAILS..... | 4 |

1 PURPOSE

- 1.1 This policy and procedure sets out the expectations at the Polytechnic Institute Australia ('PIA') for ethical and appropriate use of information technology. It should be read in conjunction with PIA's *Privacy and Personal Information Policy and Procedure*.

2 SCOPE

- 2.1 This policy and procedure applies to all students and staff at PIA, and to all use of the internet, email, social media platforms, and learning technologies.

3 POLICY STATEMENT

This policy and procedure is founded on the following principles:

- 3.1 that strategic use of information technology is an integral part of PIA's commitment to relevant, dynamic, innovative and engaging teaching practices;
- 3.2 that PIA will adopt learning technologies which enhance and support the quality of student learning and teaching activity;
- 3.3 that PIA's IT facilities are only available to authorised users;
- 3.4 that users are expected to demonstrate a respect for PIA's reputation when using its IT facilities; and
- 3.5 that all users of information technology at PIA have an obligation to behave professionally, responsibly, ethically, lawfully, and with respect for the rights and privacy of others.

4 PROCEDURES

Authorised and Unauthorised Use

- 4.1 Only authorised persons may use PIA's IT facilities. It is an offence under the *Cybercrime Act 2001* to access or attempt to access any computer system for which due authorisation has not first been obtained. Unauthorised access is prohibited by law and may result in disciplinary action and/or criminal prosecution.
- 4.2 Authorised users are determined by PIA.



Information Technology Usage Policy and Procedure

4.3 Users will only be given authorisation to use PIA'S IT facilities in order to discharge their responsibilities as members of staff, or to further their studies.

4.4 PIA may suspend or cancel the access of any user found to be in breach of the terms of this policy and procedure.

Disruption or Damage

4.5 Any potential or actual damage or disruption to PIA's IT facilities must be reported to Information Technology staff as soon as possible.

Use of Internet, Email and Social Media Platforms

4.6 PIA encourages use of the Internet and email where such use is appropriate as a student or staff member.

4.7 Users are not permitted to use PIA's internet or email for the following purposes:

- criminal or illegal activities;
- inciting or encouraging terrorism or disseminating terrorist material;
- transmitting material which could be deemed fraudulent, defamatory, profane, offensive, discriminatory, or harassing;
- making comments or using images, materials or software that might be considered offensive or abusive under Anti-Discrimination legislation and codes;
- viewing, downloading, transmitting or retaining illegal, obscene, pornographic or otherwise inappropriate material;
- disclosing private, sensitive or confidential information of a personal or organisational nature;
- sending or soliciting chain letters or spam;
- gambling; or
- accessing restricted areas of the network.

4.8 In addition, users must not:

- knowingly or maliciously interfere with PIA's IT services, network, or network infrastructure;
- compromise PIA's reputation;
- access the email account of another student or staff member; or
- place PIA in a position where liability is incurred.

4.9 Personal use of the Internet, email and social media is only sanctioned where it complies with sections 4.7 and 4.8 (above), and where such use is strictly limited, does not disrupt others, and does not place an undue burden on network resources.

4.10 Note that social media platforms are not supported by PIA's systems.

Monitoring Usage



Information Technology Usage Policy and Procedure

- 4.11 Under the *Workplace Surveillance Act 2005*, PIA may monitor or record digital communications for defined business-related purposes.
- 4.12 In the interests of ensuring compliance with this policy and procedure and related legislation, PIA reserves the right to undertake the following without notice:
- inspect, investigate, suspend, and/or terminate all email accounts;
 - block, inspect, redirect or reject any emails;
 - remove or delete any Internet resources; and
 - monitor Internet activity.

5 RESPONSIBILITIES

5.1 Users of PIA's IT facilities have a responsibility to:

- protect the privacy of their email accounts, and safeguard passwords;
- change passwords regularly;
- ensure they are using secure and approved technologies, including antivirus software;
- be careful when opening attachments or emails from unknown or unidentifiable senders;
- respect confidentiality and handle sensitive information accordingly;
- delete all personal emails and attachments once read;
- delete all unsolicited junk mail;
- ensure the content and tone of emails are appropriate and courteous;
- ensure any comment made in a private and personal capacity are explicitly designated as such;
- observe all relevant legislation, standards and codes; and
- bring any concern with respect to the Internet, email or social media to the attention of Information Technology staff as promptly as possible.

5.2 Users of PIA's IT facilities have a responsibility to ensure they do not:

- breach copyright or license provision, or copy software without the express permission of the copyright owner;
- disrupt, corrupt or destroy the work of others;
- adversely affect, damage, destroy, or place an undue burden on PIA's IT facilities, network and/or network infrastructure; or
- knowingly waste IT resources.

5.3 PIA is responsible for ensuring users are provided with a reliable and robust network service. To this end, PIA will:

- provide sufficient training in IT services and skills;
- ensure equitable access to learning technologies, the Internet and email;
- ensure students are not disadvantaged in the event of unscheduled outages; and



Information Technology Usage Policy and Procedure

- develop and implement appropriate risk management processes to minimise service disruption or outages.

6 DEFINITIONS

6.1 Terms not defined in this document may be in the PIA glossary.

Terms and definitions

IT: Information Technology.

(IT) User: a person who uses PIA's IT facilities (system, network or resources).

7 RELATED LEGISLATION AND DOCUMENTS

Documents

Privacy and Personal Information Policy and Procedure

Copyright Act 1968

Cybercrime Act 2001

Telecommunications (Interception and Access) Act 1979

Workplace Surveillance Act 2005

Higher Education Standards Framework

- 7.1 This policy and procedure complies with the Higher Education Standards Framework (Threshold Standards) 2015, Standard 2.1, which states:
2. Secure access to electronic information and adequate electronic communication services is available continuously (allowing for reasonable outages for maintenance) to students and staff during periods of authorised access, except for locations and circumstances that are not under the direct control of the provider.
- 7.2 This policy and procedure also complies with the Higher Education Standards Framework (Threshold Standards) 2015, Standard 7.3, which states:
3. Information systems and records are maintained, securely and confidentially as necessary to:
 - a. maintain accurate and up-to-date records of enrolments, progression, completions and award of qualifications;
 - b. prevent unauthorised or fraudulent access to private or sensitive information, including information where unauthorised access may compromise academic or research integrity.

8 FEEDBACK

8.1 PIA staff and students may provide feedback about this document by emailing policy@pia.edu.au.

9 APPROVAL AND REVIEW DETAILS

Created: 16 August 2018
Modified: 17 December 2019
Review Date: July 2023

Document Owner: CEO
Version: 1.3
Page 4 of 5



Information Technology Usage Policy and Procedure

| Approval and Review | Details |
|---------------------|--------------------------------|
| Approval Authority | Executive Management Committee |
| Administrator | CEO |