ASIA PACIFIC INTERNATIONAL COLLEGE

INFORMATION TECHNOLOGY SECURITY PROCEDURES

Document ID	Information Technology Security Procedures
Related Documents	Emergency Management of Information Technology Procedures Information Technology Administration Procedures
Date	16 December 2016
Date of Next Review	16 December 2018
Authorised by	Director of Accreditation, Compliance and Quality Assurance
Approved by	Executive Management Team [10 January 2017
Version	1.0
Responsible Officer	ICT Manager
References and Legislation	

Contents

1. Purpose

This procedure provides guidelines for the protection and use of information technology assets and resources within the College to ensure integrity, confidentiality and availability of data and assets.

2. Scope

All College students and employees who use or access APIC's technology equipment and/or services are bound by the conditions of these Procedures.

3. Definitions

Item	Definition
	NIL

4. Procedures

4.1 Physical Security

For all servers, mainframes and other network assets, the area must be secured with adequate ventilation and appropriate access through such as keypad, lock etc.

It will be the responsibility of the local Network Administrator to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify any member of the ICT Team immediately.

All security and safety of all portable technology, such as laptop, notepads, iPad etc. will be the responsibility of the employee who has been issued with the laptop, notepads, iPads, mobile phones etc. Each employee is required to use locks, passwords, etc. and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, the Head of ICT will assess the security measures undertaken to determine if the employee will be required to reimburse the College for the loss or damage.

All laptop, notepads, iPads etc. when kept at the office desk is to be secured by keypad, lock etc. provided by the ICT Team.

4.2 Information

All sensitive, valuable, or critical College data is to be backed-up.

It is the responsibility of the local Network Administrator to ensure that data back-ups are conducted every night and one copy of the backed up data is kept On-premises and one copy in an Offsite location.

All technology that has internet access must have anti-virus software installed. It is the responsibility of the local Network Administrator to install all anti-virus software and ensure that this software remains up to date on all technology used by the College.

All information used within the College is to adhere to the privacy laws and the College's confidentiality requirements. Any employee breaching this may have their employment terminated with the APIC or its associated colleges.

5. Technology Access

Every employee will be issued with a unique identification code to access the College technology and will be required to set a password for access every 90 days.

Each password must contain at least 9 digits and each staff member is to use a "Strong Alphanumeric" combination, which consists of lowercase letters, uppercase letters, numerals and specials characters (@, #, &, etc.) and is not to be shared with any employee within the College.

Any user violating this policy or applicable local, state, or federal laws while using the APIC Group of Colleges network shall be subject to loss of network privileges and any other disciplinary actions deemed appropriate, possibly including termination and criminal and/or civil prosecution.

The local Network Administrator is responsible for the issuing of the identification code and initial password for all employees.

Where an employee forgets the password or is 'locked out' after five attempts, then local Network Administrator is authorised to reissue a new initial password that will be required to be changed when the employee logs in using the new initial password.

The following table outlines access authorities:

Technology – Hardware/ Software	Persons/Position authorised for access
RTO Manager	• Admissions Manager and Officers • Accounts Manager and Officers • Marketing Staff • Agents • Lecturers and Teachers • Student Support Officers • Director of Accreditation, Compliance and Quality Assurance
AEI	• Admissions Manager and Officers • Marketing staff
XERO	• Accounts Manager and Officers
Westpac/HSBC Online Banking	• Accounts Manager and Officers • Financial Controller
Moodle (OHS)	• Lecturers • Students • Management • Student Administration
Office 365	• General Staff • Students • Academic Staff • Student Administration

Employees are only authorised to use College computers for personal use during their breaks and for internet usage only.

For internet and social media usage, refer to the IT, Internet, Email & Social Media Policies.

It is the responsibility of the ICT Manager to keep all procedures for this policy up to date.

6. Document Change Control

Version	Change Description	Date	Author
1.0	Placed in new policy format	16 December 2016	Corinne Green