ASIA PACIFIC INTERNATIONAL COLLEGE

BRING YOUR OWN MOBILE DEVICE GUIDELINES

Document ID	Bring Your Own Device Guidelines
Related Documents	Technology Hardware Purchasing Procedures Use of Software Procedures Delegations Policy IT, Internet and Social Media Guidelines
Date	13 December 2016
Date of Next Review	13 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

ASIA PACIFIC INTERNATIONAL COLLEGE

1. Purpose

At APIC, we acknowledge the importance of mobile technologies in improving College communication and productivity. In addition to the increased use of mobile devices, employee members have requested the option of connecting their own mobile devices to APIC's network and equipment. We encourage you to read this document in full and to act upon the recommendations. These guidelines should be read and carried out by all employee.

2. Scope

This document provides guidelines for the use of personally owned notebooks, smart phones, tablets and other types of mobile devices for College purposes. All students and employees who use or access APIC's technology equipment and/or services are bound by the conditions of this Policy.

3. Definitions

Item	Definition
	NIL

4. Approved Mobile Devices

Current mobile devices approved for College use are:

- Notebooks;
- Laptops;
- Smart phones; and
- Tablets

5. Use of Personal Mobile Devices

Each student or employee who utilises personal mobile devices for College use agrees to:

- Not download or transfer College or personal sensitive information to the device. Sensitive information includes, but not limited, to intellectual property, other employee details, financial documents and other information;
- Not use the personal mobile device as the sole repository for APIC's information. All College information stored on mobile devices should be backed up;
- Make every reasonable effort to ensure that APIC's information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorised persons and all registered devices should be password protected;

- Maintain the device with the latest available operating system and current security software;
- Not share the device with other individuals so as to protect any College data accessed through the device;
- Abide by APIC's internet policy for appropriate use and access of internet sites etc.;
- Notify APIC immediately in the event of loss or theft of the registered device
- Not to connect USB memory sticks from an untrusted or unknown source to APIC's equipment.

All employees who have a registered personal mobile device for College use acknowledge that the College:

- Owns all intellectual property created on the device
- Can access all data held on the device, including personal data
- Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data
- Has the right to deregister the device for College use at any time.

6. Keeping Mobile Devices Secure

The following must be observed when handling mobile computing devices (such as notebooks and iPads):

- Mobile computer devices must never be left unattended in a public place, or in an unlocked house, or in a motor vehicle, even if it is locked. Wherever possible they should be kept on the person or securely locked away;
- Cable locking devices should also be considered for use with laptop computers in public places, e.g. in a seminar or conference, even when the laptop is attended; and
- Mobile devices should be carried as hand luggage when travelling in aircraft.

7. Exemptions

These guidelines are mandatory unless a member of the Executive Management Team grants an exemption. Any requests for exemptions from any of these directives, should be referred relevant employee's Executive Management Team member.

8. Breaches

Any breach of this policy will be referred to the employee line-manager who will review the breach and determine adequate consequences, which could include the confiscation of the device and/or termination of employment.

9. Indemnity

APIC bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of employee in accessing or using these resources or facilities. All employee indemnify APIC against any and all damages, costs and expenses suffered by APIC arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by APIC.

10. Document Change Control

Version	Change Description	Date	Author
1.0	Placed in new policy format	13 December 2016	Sachin Tandular