ASIA PACIFIC INTERNATIONAL COLLEGE

EMERGENCY MANAGEMENT OF INFORMATION TECHNOLOGY PROCEDURES

Document ID	Emergency Management of Information Technology Procedures
Related Documents	ICT Disaster Recovery Plan ICT Management Plan
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....2
2. Scope....2
3. Definitions....2
4. Procedures....2
4.1 IT hardware failure....2
4.2 Virus or other security breach....2
5. Website Disruption....2
6. Document Change Control....3

APIC
ASIA PACIFIC INTERNATIONAL COLLEGE

1. Purpose

This guideline outlines the emergency management of all information technology within the College.

2. Scope

All 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 IT hardware failure

Where there is failure of any of the College's hardware, this must be referred to the local Network Administrator immediately.

In the event of IT hardware failure, it is the responsibility of the Network Administrator to

- Capture data at the time of the failure
- Capture (when possible) utilisation data through user's factory tracking system
- Make failure and utilisation data available to the supplier (if applicable)
- Contain the damage and minimise risks

It is also the responsibility of the Network Administrator, undertake tests on planned emergency procedures, every quarter to ensure that all planned emergency procedures are appropriate and minimise disruption to College operations.

4.2 Virus or other security breach

In the event that the College's information technology is compromised by software virus or other relevant possible security breaches, such breaches are to be reported to the Head of ICT and Administration immediately.

The ICT Manager is responsible for ensuring that any security breach is dealt with within 2 hours to minimise disruption to College operations.

5. Website Disruption

In the event that College website is disrupted, the following actions are to be undertaken immediately:

- ICT Team Leader must be notified.
- ICT Team Leader to check configuration in web hosting company. For any issues, contact the provider. For internal issues, escalate for Systems Administrator.
- ICT Team Leader to contact Sitelock.

6. Document Change Control

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