Australian and New Zealand College of Anaesthetists
INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY POLICY

1. PURPOSE

This policy sets out guidelines for protecting the security of the College's information and communications technology resources ("**ICT Resources**")

The scope of this policy includes all individuals using the College's ICT Resources including employees, contractors, volunteers, Fellows, international medical graduate specialists (IMGS) and trainees.

2. INTRODUCTION

The College provides a variety of ICT Resources to support the activities of the College. These include, but are not limited to:

- the College's voice and data network, including fixed, wireless and mobile network services;
- the learning management system (Networks);
- the training portfolio system (TPS);
- the continuing professional development (CPD) system;
- the exam management system (EMS);
- the ANZCA portal and online event registration system;
- iMIS, the College's core database of record;
- Informz, the College's electronic newsletter and survey tool
- computer hardware and software, including personal computers, notebooks, servers and printers;
- internet access, including wireless internet access;
- mobile phones, smart phones and wireless data cards; and
- email, telephones and related communications services.

Version 1.0
Last updated: Apr 9, 2016
Amended: SPO&T Unit
Approval: Council
Approved: FINAL

The College's ICT Resources are valuable and often store or process sensitive or confidential information regarding the College and its stakeholders. As a result it is important that everyone looks after the security of ICT Resources carefully.

3. BODY OF POLICY

The College's ICT Resources includes equipment such as computers, notebooks, servers and smartphones. This ICT equipment may contain sensitive or confidential information. All individuals using College ICT equipment have a responsibility to protect it from theft, unauthorised access, loss or damage.

3.1 Access to ICT Resources

- Access to the College's ICT Resources will be by username and password. You must not share your password with others and you must change your password regularly.
- Confidential information must be stored in such a way to ensure that only authorised persons can access it.
- You must not remove ICT equipment from the College without prior authorisation from the IT Operations Manager.
- Access to work areas containing ICT equipment is restricted to those with the appropriate access cards during business hours and may only be accessible by authorised individuals after hours.
- Before leaving your workstation for any period of time, ensure that your computer is either locked or switched off, to help protect from unauthorised access.
- The College may install security software to protect ICT Resources from unauthorised access or damage. You must not interfere with or try to bypass this software.
- Access to ICT equipment may be monitored and access records may be maintained by the College.

3.2 Wireless network access

The College provides wireless network access within the College's office. Connecting unauthorised devices may compromise the network and is not permitted.

3.3 Portable ICT Resources

If you are issued with portable ICT equipment, such as a mobile phone or laptop, you are responsible for ensuring that it is kept safe at all times. Do not leave such equipment unattended.

If you suspect an item has been lost or stolen, report this immediately to the IT Operations Manager and (if applicable) to the police.

If an item you are issued with is lost or stolen due to your negligence, you may be required to reimburse the College.

3.4 Business continuity

The College will regularly back-up its major systems to ensure there is minimal disruption to ICT Resources in the event of a power outage or other problem. However the College recommends you save your work regularly to avoid losing any progress.

3.5 Disposal of ICT Resources

You must not dispose of any College ICT Resources without authorisation from the IT Operations Manager. You must ensure that all data is removed from the equipment prior to disposal. Software must also be removed to prevent potential breaches of software licence agreements.

3.6 Breaching this policy

Suspected breaches of this policy may result in withdrawal of your access to College ICT Resources.

If you are found to have breached this policy you may be subject to disciplinary action. For employees or contractors, depending on the nature of the breach, this may include termination of your employment or engagement with ANZCA.

Suspected criminal offences, such as theft, will be reported to the police.

4. CONCERNS OR COMMENTS

If you have any concerns about the ICT security policy please contact the IT Operations Manager on +61 3 9510 6299 or via servicedesk@anzca.edu.au . Requests must be in writing and resolution of concerns will be sought as promptly as possible.

5. CHANGES TO ANZCA ICT SECURITY POLICY

The College may modify or amend this policy at any time. Formal notice of amendments will not ordinarily be given, but the current ICT security policy will be available via the College website www.anzca.edu.au or College corporate policy register (G:\Policies) or by contacting the College on +61 3 9510 6299.

6. RELATED DOCUMENTS

- ANZCA ICT Code of Conduct Policy
- ANZCA ICT Mobile Phone Policy
- ANZCA Electronic Communications Policy
- ANZCA Social Media Policy – Staff
- ANZCA Social Media Policy – Fellows, IMGS and trainees

7. CHANGE CONTROL REGISTER

Version	Author	Approved by	Approval Date	Sections Modified
1.0	Strategic Project Office & Technology	Council	April 9, 2016	Created