

Australian and New Zealand College of Anaesthetists INTERNET, EMAIL AND COMPUTER USE POLICY

1. PURPOSE

The College recognises the usefulness of the internet, email, mobile devices and computer equipment as research, communication and work tools. This policy sets out the appropriate standards of behaviour for users of the College's information technology resources.

2. INTRODUCTION

At all times when accessing or using the College's information technology resources, users must ensure that they comply with this policy. It is the user's responsibility to ensure that they use the College's information technology resources in a lawful and professional manner.

This policy outlines the expectations in the use of the College's:

- 3.1 Information technology resources.
- 3.2 Internet.
- 3.3 Social media.
- 3.4 Email facilities.
- 3.5 Mobile phones and mobile devices.

If a user is unsure about any matter covered by this policy, they should seek the assistance of their manager, committee chair, the chief executive officer or the president.

2.1 Scope

This policy applies to all staff members of the College, Fellows, trainees, volunteers and contractors (including sub-contractors and temporary contractors) referred to as **users**.

This policy applies to the use of all internet, email and computer facilities, both during and outside of business working hours. This policy applies to the use of internet, email and computer facilities inside the workplace, as well as use from remote locations. Use of computer facilities includes use of laptops, mobile phones and similar products, and any other equipment that provides a means of accessing the College's email and internet facilities. For example, this policy extends to the use of a personal computer which has access to the College's IT systems.

3. BODY OF POLICY

3.1 Information technology resources

The College's information technology resources ("IT resources") are provided to support the business and administrative activities of the College. These resources include:

- The College's network.
- Computer systems and software including personal computers, notebooks and servers.
- Mobile phones, smart phones and wireless data cards.
- Access to the internet.
- Email, telephones and related services.

If users produce, collect and/or process College related information in the course of their work, that information remains the property of the College. This includes information stored on third party websites.

3.1.1 Extent of personal use

Users are permitted to use the College's IT resources for limited, incidental personal purposes, provided that such use does not:

- Interfere with the efficient business operations of the College.
- Violate this policy or any other policy of the College.
- Negatively impact upon the user's work performance.
- Hinder the work of other users.
- Damage the reputation, image or operations of the College.
- Such use must not cause noticeable additional cost to the College.
- The College accepts no responsibility for:
 - Loss or damage or consequential loss or damage, arising from personal use of its IT resources.
 - Loss of data or interference with personal files arising from the efforts to maintain the IT resources.

3.1.2 Guidelines for use of IT resources

Users must comply with the following guidelines when using the College's IT resources:

- Users must use their own username/login code and/or password when accessing the College's computer systems.
- Users should protect their username/login code and password information at all times and not divulge such information to any other person, unless it is necessary to do so for legitimate business reasons.
- Username/login codes and passwords are not to be recorded on or near computer equipment/mobile devices.
- Users should ensure that they log off from their account, and lock their computer/mobile device or shut down their computer/mobile device when leaving such equipment unattended to ensure that others do not have access to the College's computer systems.

- Users in possession of the College's computer equipment or mobile devices (including laptops, mobile phones, pagers, personal data assistants, wireless data cards, etc) must at all times ensure that such equipment is stored or placed in areas with a minimal possibility of theft or damage.
- IT resources must not be used for private commercial purposes except where the paid work is conducted in accordance with the College's practice, or the work is for the benefit of an entity in which the College holds an interest.
- Use of proprietary software is subject to terms of license agreements between the College and the software owner or licensor, and may be restricted in its use.
- The ANZCA name or logo may only be used with prior approval from the general manager, communications.

All use must be in accordance with the prior approval of the Communications Department.

3.1.3 Prohibited conduct

Certain behaviour is considered to be inappropriate use of the College's IT resources and is strictly prohibited. Examples of such prohibited conduct are, but are not limited to:

- a) Users must not send (or cause to be sent), upload, download, use, retrieve, or access any file, email or internet material that:
 - I. Is obscene, offensive or inappropriate. This includes text, images, sound or any other material, sent either in an email or in an attachment to an email, or through a link to an internet site (URL). For example, material of a sexual nature, hateful, indecent or pornographic material.
 - II. Causes insult, offence, intimidation or humiliation by reason of unlawful harassment or discrimination.
 - III. Is defamatory or incurs liability or adversely impacts on the image of the College. A defamatory message or material is a message or material that is insulting or lowers the reputation of a person or group of people.
 - IV. Is otherwise illegal, unlawful or inappropriate.
 - V. Affects or may affect the performance of, or cause damage to or overload the College's computer systems or internal or external communications in any way.
 - VI. Gives the impression of or is representing, giving opinions or making statements of on behalf of the College without the express authority of the College.

- b) Users must not use IT resources to:
- I. Violate copyright or other intellectual property rights. Computer software that is protected by copyright is not to be copied from, or into, or by using the College's computing facilities, except as permitted by law or by contract with the owner of the copyright. Similarly, users should not copy or access copyright protected music or videos on the College's IT resources.
 - II. Breach an individual's privacy, including patients under the care of a Fellow or trainee;
 - III. Create any legal or contractual obligations on behalf of the College unless expressly authorised by the College.
 - IV. Disclose any confidential information of the College or any employee, Fellow, trainee, client or supplier of the College unless expressly authorised by the College.
 - V. Install software or run unknown or unapproved programs on the College's computers. Under no circumstances should users modify the software or hardware environments on the College's computer systems (this includes installing software purchased by users for personal private use) without prior approval from the general manager, IT.
 - VI. Gain unauthorised access (hacking) into any other computer within the College or outside the College or attempt to deprive other users of access to or use of any College computing system.
 - VII. Plagiarise another person's work.
 - VIII. Deliberately send or cause to be sent chain or spam emails in any format.
 - IX. Obtain personal gain. For example, running a personal business using the College's computers.
 - X. Gamble.
 - XI. Stream content for personal use.
 - XII. Use peer to peer file sharing software such as VUZE, BitTorrent, etc.
 - XIII. Download, install or use instant messaging software.
 - XIV. Perpetrate any form of fraud or software, film or music piracy.
- c) Users must not use another user's computer or internet access or email facilities (including passwords and usernames/login codes) for any reason without the express permission of the user.

3.2 Internet

The College's IT resources should only be connected to the internet using means authorised by the general manager, IT.

Users are not permitted to publish personal web pages on computers connected to the ANZCA network.

3.3 Social media

Staff members are not permitted to "recommend" their current or former college co-workers for professional networking websites which would identify the College as the user's employer (such as "LinkedIn") without prior approval from the Human Resources Department.

The College's IT resources are provided for work purposes. Access to social networking websites is not deemed a requirement of most positions. However, if a user is permitted to access social networking websites, the user is responsible for ensuring that their access does not:

- Interfere with the efficient business operations of the College.
- Violate this policy or any other policy of the College.
- Negatively impact upon the user's work performance.
- Hinder the work of other users.
- Damage the reputation, image or operations of the College.

For the sake of clarity, social media includes, but is not limited to:

- Social networks (such as Facebook and MySpace).
- Blogs.
- Wikis (such as Wikipedia).
- Podcasts.
- Forums.
- Content communities (such as YouTube and Flickr).
- Microblogs (such as Twitter).

Users must take a common sense approach to the content that they publish online. Because of the public nature of the internet and social media, this common sense approach also applies to use of social networking sites outside of business hours or on equipment other than College equipment.

If a user is holding themselves out as a representative of the College, any material published online must:

- Be relevant to the user's area of expertise.
- Not be anonymous.
- Maintain professionalism, honesty and respect.

Statements of fact about the College and its products and services, publicly available information and information already published on the College's website are all examples of appropriate online content.

Users must not publish any material online that contains the College's confidential information (including financial information and information about organisational matters), the personal information of another (without that individual's consent), information about the College's customers or clients, or content that may offend, intimidate, defame or humiliate a Fellow, trainee, staff member, volunteer or contractor of the College. Further, if a user becomes aware of the publication of material that is linked to the College, its workers or its clients which would be deemed distasteful or inappropriate, the user should report such conduct to the College's Human Resources Department.

If a user is unsure about whether they should publish material on the internet, they should seek guidance from the general manager, IT.

3.4 Email

Appropriate standards of civility should be used when using email and other messaging services to communicate with other staff members or any other message recipients. When using the email or messaging system users must not send:

- Angry or antagonistic messages – these can be perceived as bullying or threatening and may give rise to formal complaints under grievance procedures or discrimination/sexual harassment procedures.
- Offensive, intimidating or humiliating emails – the College's IT resources must not be used to humiliate, intimidate or offend another person/s on the basis of their race, gender, or any other attribute prescribed under anti-discrimination legislation.

3.4.1 Guidelines for use of the College's email system

A user must comply with the following guidelines when using the College's email system:

- Any disclaimer which is automatically included in the College's emails must not be removed.
- If a user receives an email which they suspect contains a virus, they should not open the email or any attachment to the email and should immediately contact the IT service desk for assistance.
- If a user receives an email the content of which (including an image, text, materials or software) is in breach of this policy or any the College's other policies, the user should immediately delete the email and report the matter to the general manager, IT. The user must not forward the email to any other person.
- Users must not publish their college email address on a private business card.
- Users must not forward or copy emails that contain personal information about an individual without the prior permission of that individual.
- Users must adhere to the guidelines and prohibitions set out in this policy at all times.
- Messaging and email must not be used for private commercial purposes except where the work is for the purposes of a corporate entity in which the College holds an interest.

3.5 Mobile phones and mobile devices

Mobile phones and/or mobile devices may be provided by the College to staff members, Fellows or trainees for the purposes of carrying out college business. Requests for a College mobile phone and/or mobile device must be sent to the IT Department.

Mobile phones, mobile devices, accessories and associated telephone numbers remain the property of the College at all times.

Mobile phones and mobile devices are considered IT resources and, as such, their use is governed by this policy.

Users are responsible for understanding the costs associated with using the College's mobile phones and mobile devices and should ensure that this equipment is used in the most cost effective manner. All costs associated with the use of mobile phones and mobile devices will be included in the appropriate management budget reports. Periodic checks and trend analysis will be undertaken by the IT Department on all costs associated with the use of mobile phones and mobile devices. An investigation may be undertaken where it is identified that a user is exceeding reasonable personal use of the equipment provided.

3.5.1 Guidelines for use of the College's mobile phone and mobile devices

Users must comply with the following guidelines when using the College's mobile phones and mobile devices:

- Users must maintain the operational effectiveness of the mobile phone or mobile device (i.e. keeping the batteries charged when required to be contacted).
- Mobile phones and mobile devices that have the ability to be password protected and encrypted must have this security feature activated at all times. Users are not to remove or modify such security features as configured by the IT Department.
- International and premium number call facilities will not be available without prior agreement for both business and private use and must be approved by the budget holder for the phone. Requests to allow international use should be made through the IT service desk.
- Users are prohibited from using mobile phones or devices while operating a motor vehicle in the conduct of business for the College.
- Users must report any loss, theft, damage or security breach of any mobile phone or mobile device immediately to the IT Department to ensure appropriate measures are taken to secure and disable the device. If such loss, theft or damage is due to the negligence of the user, the user may be responsible for the cost of replacing or repairing the mobile device.

4. MONITORING – EMAIL, FILES, INTERNET DOWNLOADS OR DATA STORAGE

The College does not generally monitor email, files, internet downloads or data stored on its IT resources. However, the College reserves the right to access and monitor any computer or other electronic device connected to the College's network. This includes equipment owned by the College and personal computing equipment (for example, laptops) that are connected to the network.

Access to and monitoring of equipment is permitted for any reason, including but not limited to, suspected breaches of this policy by a user or unlawful activities. Access to and monitoring includes, but is not limited to, email, web sites, server logs and electronic files.

ANZCA may keep a record of any monitoring or investigations.

5. BREACH OF THIS POLICY

Where the College suspects or finds evidence of a breach of this policy, the College reserves the right to restrict a user's access to its IT resources.

Any user found to have violated this policy may be subject to disciplinary action.

Criminal offences will be reported to the police.

6. CONCERNS OR COMMENTS

If you have any concerns about the internet, email and computer use policy please contact the IT service desk 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.

7. CHANGES TO ANZCA INTERNET, EMAIL AND COMPUTER USE POLICY

The College may modify or amend this policy at any time. Formal notice of amendments will not ordinarily be given, but the current internet, email and computer use policy will be available via the College website. The latest version of the policy can be accessed via the College website www.anzca.edu.au or by contacting the College on +61 3 9510 6299.

8. ASSOCIATED POLICIES AND LEGISLATION (INCLUDING GUIDELINES & PROCEDURES)

College policies:

- Code of conduct
- Discipline and termination policy
- Discrimination prevention policy
- Privacy policy
- Sexual harassment policy
- Workplace health and safety policy
- Workplace bullying and violence prevention policy

Legislation:

- Copyright Act 1968 (Cth)
- Disability Discrimination Act 1992 (Cth)
- Equal Opportunity Act 2010 (Vic)
- Fair Work Act 2009 (Cth)
- Privacy Act 1988 (Cth)
- Racial Discrimination Act (1975 (Cth)
- Sex Discrimination Act 1995 (Cth)
- Trade Marks Act 1995 (Cth)
- Trade Practices Act 1974 (Cth)

9. FURTHER INFORMATION AND ASSISTANCE

Adherence to this policy will generally ensure compliance with the requirements of ANZCA and legislation. However, there may be instances where inadvertent breaches could occur. When in doubt users requiring assistance with interpretation of the policy, or who wish to report a breach of this policy, should contact the IT service desk.

10. CHANGE CONTROL REGISTER

Version	Author	Approved by	Approval Date	Sections Modified
1	Information Technology Unit	Council	Nov 11, 2011	Created