Australian and New Zealand College of Anaesthetists
ACCEPTABLE USE OF ICT RESOURCES POLICY

1 Purpose

This policy sets out the appropriate standards of behaviour for anyone using ANZCA's information and communications technology (ICT) resources.

The purpose of this policy is to:

- establish standards for acceptable use of ANZCA ICT resources and information.
- regulate the access to ANZCA ICT resources; and
- ensure protection of information held within ANZCA environments.

Permission to use ANZCA ICT resources is contingent upon compliance to this policy. This policy must be reviewed in conjunction with the ANZCA Privacy Policy and ANZCA Information Security Policy.

1.1 Scope

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

- the voice & data network, including fixed, wireless & mobile network services.
- the learning management system,
- 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 records,
- Informz, the College's electronic newsletter and survey tool, computer hardware and software, including personal computers, notebooks, and servers,
- Zoom for communication and video conferencing,
- Microsoft productivity suite for content development, communication, document management, and collaboration,
- internet access, including wireless internet access,
- mobile phones, smart phones, and wireless data cards, and
- other services for specific use-cases across the business.

This policy applies to:

a) all technology resources used by, operated by, or provided on behalf of ANZCA;

b) all information collected, created, stored, or processed by, or for ANZCA on our information systems and infrastructure;

c) all locations and times when ANZCA ICT resources are used. It applies when using ANZCA resources during or outside business hours, on College property or offsite.

d) all individuals who utilise, or are involved in deploying and supporting, information systems and resources provided by ANZCA. This includes all staff (full-time, part-time,

casual), contracted and agency staff, trainees, volunteers, Fellows, specialist international medical graduate (SIMGs), suppliers, partners, contractors, sub-contractors, or affiliated organisations who use ANZCA ICT Resources; and

e) all external suppliers contracting with ANZCA and any of their personnel accessing the ANZCA ICT resources including the internet, or other resources authorised for official use. This includes any person working in a permanent, temporary, casual, contracted, voluntary or honorary capacity.

2 Policy

2.1 Acceptable Use

All individuals who access, use, or otherwise engage with ANZCA ICT resources must:

a) respect the rights of all individuals, including other users;

b) only use ANZCA ICT resources for authorised purposes, and not in breach of relevant laws or contractual obligations;

c) not use ANZCA equipment, systems and infrastructure for non-commercial personal purposes beyond a reasonable amount, or to the detriment of ANZCA or its goals;

d) not access, distribute, store or display illegal, pirated or offensive material;

e) not use ANZCA equipment, systems or infrastructure for unauthorised personal financial or commercial gain;

f) If issued with a portable equipment such as a mobile phone or laptop, it is the responsibility of the owner to ensure the device is kept safe at all times. Equipment must be locked when left unattended or in public.

g) not misrepresent the views of ANZCA, via use of ANZCA ICT resources;

h) not use generative AI and large language models for work related content generation and evaluation without appropriate internal consultation and risk assessment;

i) not conduct activities that consume excessive network bandwidth;

j) maintain the security and confidentiality of information generated or collected by ANZCA in accordance with the ANZCA Privacy Policy.

k) only load corporate data essential to their role onto their mobile device(s).

l) not load pirated software or illegal content onto their devices.

m) only install applications from official and approved sources. Installation of code from untrusted sources is forbidden. ICT must be consulted if unsure if an application is from an approved source.

n) keep devices up to date with manufacturer or network provided patches. As a minimum, patches should be checked weekly and applied at least once a month.

o) not connect devices to a PC which does not have up to date and enabled anti-malware protection and which does not comply with ANZCA policies.

p) ensure devices are encrypted per best practice.

q) not merge personal and work email accounts on their devices. They must take particular care to ensure that ANZCA data is only sent through the ANZCA email system. If a user suspects that ANZCA data has been sent from a personal email account, either in body text or as an attachment, they must notify ICT immediately.

r) ensure backup of their own personal data. ANZCA will not accept responsibility for the loss of files due to a non-compliant device being wiped for security reasons.

s) not use corporate workstations to backup or synchronize device content such as media files unless such content is required for legitimate business purposes.

t) ensure that any 3rd party personal devices not issued by ANZCA have up-to-date anti-malware and threat protection at all times.

u) always verify the authenticity of an email, text, and telephone call. Mobile devices only show the user's name and not the actual email address from which a message was sent. These names are often spoofed to mimic someone known and trusted.

v) never click links in emails or text messages from untrusted sources. Users must verify the source of messages even with trusted sources.

w) keep a close eye on URLS, avoid advertisements, giveaways, 'free' applications that are likely too good to be true. These could be phishing sites used to steal information.

x) verify callers' information recognising many scams involve spoofing Banks, ATO, or Social Security Administration asking for personal banking information.

y) be cautious of accepting disclaimers and authorising permissions given to applications to read and harvest information on personal devices including text messages, contact lists etc. Many free applications use this information to mine or sell data.

z) when discarding used technology, users must follow manufacturer recommendations on how to wipe the technology so personal data doesn't fall into untrusted hands.

Users must report suspected or actual security breaches to the Information Technology Service Desk (ITSD) in a timely manner.

The above requirements will be checked regularly, and should a device be non-compliant, may result in the loss of access to email, a device lock, or in particularly severe cases, a device wipe. Non-compliance with ANZCA policy will imply a compliance breach and result in the loss of access to ANZCA ICT resources.

2.2 Instances requiring immediate action

The following instances may require a full or partial wipe of the device, or other appropriate intervention:

a) A user has exceeded the maximum number of failed password attempts.

b) A device is jailbroken/rooted or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed or suspected to have allowed unauthorized access to company data

c) A device contains an app known to contain a security vulnerability (if not removed within a given timeframe after informing the user).

d) A device is lost or stolen. Users must report suspected lost or stolen equipment immediately to the Information Technology Service Desk (ITSD) and (if applicable) to the police. If lost or stolen due to the owner's negligence, they may be required to reimburse the College.

2.3 Secure System Access and Use

To protect access to ANZCA ICT Resources, individuals are required to:

a) select strong passwords that are not easily discoverable;

b) securely store passwords that provide access to ANZCA systems or information;

c) only use the accounts provided by ANZCA for own individual use;

d) not share ANZCA-provided or self-selected passwords with other individuals;

e) keep personal and ANZCA-provided systems, used to access ANZCA information, free from known vulnerabilities by keeping up-to-date with authorised security updates;

f) maintain operational and up-to-date antivirus on personal and ANZCA-provided systems used to access ANZCA information;

g) not bypass or attempt to circumvent the ANZCA Security Controls or Protection Mechanisms;

h) not introduce malicious software such as viruses, worms, ransomware or trojans into the ANZCA environment; and

i) not use Hacking Tools (including sniffing, scanning, password guessing or exploitation) when accessing using or otherwise engaging with ANZCA ICT resources.

j) notify ANZCA of any device, account, or system compromise as soon as identified.

k) if using a personal device or non-ANZCA device to access ANZCA resources:

- Ensure that the device is always stored securely whilst accessing and/or storing ANZCA information
- Ensure that the device is password protected to the extent necessary to ensure that no third party can access ANZCA ICT resources or ANZCA information; and
- Immediately notify ANZCA of any breach of the Privacy Policy, and/or of any unauthorised access to ANZCA ICT resources or ANZCA confidential information (including resident information).
- Ensure that post-incident corrective actions are taken to immediately remediate information security compromise.
- Comply with all reasonable requests made by ANZCA and do all things reasonably required by ANZCA to ascertain the extent of any Privacy and/or security breach and to remedy the consequences of any such breach, including (without limitation):
    - providing ANZCA with such information as it requires to ascertain the extent to which the security/integrity of any device has been compromised and ANZCA confidential information (including resident information) has been disseminated to third parties; and
    - Within 24 hours of request being made, providing ANZCA with evidence of corrective actions taken to address any security breach and/or exposure of device/systems and to remedy the same, and comply with consequences of the same.
- Ensure that the personal device otherwise always complies with this policy whilst accessing ANZCA ICT Resources and/or storing any ANZCA information (including resident information).
- Destroy and/or permanently remove access to ANZCA ICT resources from all devices once it ceases being a provider/supplier to ANZCA, save to the extent required to comply with its contractual obligations to ANZCA, in which case the provision of this policy will continue to apply.
- Destroy and/or permanently remove any ANZCA confidential information from all devices once it ceases being a provider/supplier to ANZCA, information which is not of and incidental to the services provided by the Provider and not otherwise a record required to be preserved by law. Any ANZCA confidential information retained by the Provider on devices will continue to be dealt with in strictly

compliance with the ANZCA ICT resources Policy and the confidentiality obligations contained within the Providers contract with ANZCA.

- Ensure that all external suppliers and partners, their staff, agents, and employees who access the ANZCA ICT resources are aware of and comply with this policy and if required by ANZCA, execute, and deliver to ANZCA written acknowledgement that it, they, he or she has received a copy of this policy and is bound by its terms.

2.4 Monitoring and Compliance

a) The College monitors its information systems for compliance with this Policy. It records the use of its ICT Resources, including by recording internet sites accessed, recording all emails received and sent (including deleted emails) and accessing data on any device connected to the network.

b) ANZCA may refer serious matters or repeated breaches to appropriate external authorities which may result in disciplinary and / or civil, and / or criminal proceedings.

c) ANZCA has a statutory obligation to report illegal activities and corrupt conduct to appropriate authorities and will cooperate fully with the relevant authorities. Suspected criminal offences will be reported to the police.

d) Any information the College discovers while monitoring ICT Resources may be used or disclosed:

- as part of investigations into suspected inappropriate conduct, including suspected breaches of College policy;
- as evidence in legal proceedings;
- for purposes related to engagement of its employees or contractors;
- for purposes related to membership of the College by fellows and trainees;
- for the purpose of law enforcement (for example, in cases of alleged fraud or theft);
- to avoid a threat of injury to a person or damage to property.

e) The following consequences apply when a breach of this policy occurs.

- The college may restrict or suspend your access to the college's ICT Resources at any time if it suspects you may be involved in a breach of College policy or other inappropriate behaviour.
- Depending on the nature of the breach, disciplinary may be action taken which may include termination of your employment or engagement with the College. To the extent allowed by law, ANZCA is not liable for loss, damage or consequential loss or damage arising directly or indirectly from an individual's use or misuse of any ICT resources.

3 Definitions

The following definitions apply for the purpose of this Policy:

a) Authorised Purposes means activities associated with work at ANZCA, or provision of services to or by ANZCA, which are approved or authorised by the relevant officer or employee of ANZCA in accordance with ANZCA policies and procedures or pursuant to applicable contractual obligations, limited personal use, or any other purpose authorised by the relevant officer or employee.

b) Hacking Tools means tools that are designed to facilitate the identification and exploitation of software or system weaknesses for the purposes of unauthorised access.

c) ICT resources, or ICT resources, includes, but is not limited to:

- All computers and all associated data networks and systems, internet access and network bandwidth, email, hardware, data storage, computer accounts, all systems, media, software (both proprietary and those developed by ANZCA) and telephony services.
- Information Technology services provided by third parties that have been engaged by ANZCA.
- Information Technology services provided jointly, or as part of a joint venture between ANZCA and a subsidiary organisation owned by ANZCA or any other partner organisation.

d) Security Controls are people, process and technology interventions designed to identify, protect, detect, respond, and recover from security events and incidents.

e) 'Misuse' includes, but is not limited to:

1. breaching ANZCA Privacy Policy or ANZCA Code of Conduct;
2. use of ANZCA ICT resources for illegal activities including:
    - intentional damage of facilities;
    - breach of copyright;
    - sending unsolicited commercial email;
    - using college computers and networks for unauthorised access, interception, data/system interference to computers and networks breaching the Crimes Act;
    - theft of equipment, software or data;
    - creation, possession or distribution of offensive content and pornography;
    - unauthorised surveillance of employees;
    - sending offensive emails, displaying inappropriate screen saver images and accessing inappropriate material which may inadvertently be observed by others;
    - cyberstalking or cyberbullying; and
    - any other unlawful activity.
3. use that causes or contributes to a breach of any provision of a law, statute, regulation, subordinate instrument or code of practice or conduct applying to ANZCA or to which users are subject;
4. use that contravenes a ANZCA statute, regulation, rule, policy, procedure, or values;
5. creating, transmitting, storing, downloading or possessing illegal material;
6. accessing, displaying, copying, downloading, distributing, storing or sharing pirated software, games, video, music, images, fonts, or other copyright material;
7. the deliberate or reckless creation, transmission, storage, downloading, or display of any offensive or menacing images, data, or other material, or any data capable of being resolved into such images or material, except in the case of the appropriate use of ICT resources for ANZCA work purposes;
8. use which constitutes an infringement of any intellectual property rights, or copyright of another person or organisation;
9. communications which would be actionable under the law of defamation;
10. communications which misrepresent a personal view as the view of ANZCA;
11. use which constitutes unauthorised recording, publishing, or communication of ANZCA communications, meetings, or conversations;

12. deliberate or reckless undertaking of activities resulting in any of the following:
    - the imposition of an unreasonable burden on ANZCA ICT resources;
    - corruption of or disruption to data on ANZCA ICT resources, or to the data of another person or organisation;
    - disruption to other Authorised Users; or
    - introduction or transmission of any hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs in any form including hyperlinks, executable code, scripts, active content, and other software into ANZCA ICT resources.
13. circumventing authentication or access control measures, security or restrictions upon the use of any ICT resources or account, including the unauthorised distribution or use of tools for compromising security, including but not limited to password guessing programs, cracking tools, packet sniffers or network probing tools;
14. betting online or gambling, other than participation in approved competitions where the primary purpose is social rather than financial;
15. use of any ICT resources for sending junk mail or unsolicited bulk messages without ANZCA approval, for-profit messages, or chain, hoax or scam letters or messages;
16. use of any ICT resources for the purposes of any private business whether for profit or not, or for any business purpose other than ANZCA business, without prior approval from authorised personnel;
17. subscribing to list servers, mailing lists and other like services for purposes other than ANZCA work or study or limited personal use;

    participation in online conferences, chat rooms, discussion groups or other like services for purposes other than ANZCA work or study or limited personal use;
18. unauthorised accessing of information, including but not limited to unauthorised access to servers, hard drives, email accounts or files;
19. unauthorised reserving of, or exclusion of others from using, any ICT resources;
20. performing an act which will interfere with the normal operation of any ICT resources;
21. unauthorised use of ANZCA logo;
22. representing that a message or material comes from another person without that person’s authorisation;
23. knowingly running, installing or distributing on any ICT resources a program intended to damage or to place excessive load on any ICT resources, including without limitation programs in the nature of computer viruses, Trojan horses and worms;
24. failure to comply with the conditions of use imposed by an external provider when that provider's equipment or services are used in conjunction with any ICT resources;
25. providing a password or other means of authentication for any ICT resources to another person without prior written approval from authorised ANZCA personnel, or failing to take reasonable care to protect a password or other means of authentication for any ICT resources from being accessed or used by another person;

26. failing to exercise reasonable care in the use, management and maintenance of ICT resources, including but not limited to taking reasonable steps to ensure security and integrity of ICT resources, including protection of equipment, systems and data from theft, unauthorised use or viruses;
27. failing to comply with any reasonable instruction given by or with the authority of ANZCA authorised personnel to remove or disable access to material;
28. using computing processing resources owned or operated by ANZCA or computer resources powered by electricity provided by ANZCA to perform mining of cryptocurrencies or brute forcing of cryptographic hash values for personal gain;
29. aiding, abetting, counselling or procuring a person to do any of the things referred to above;
30. inducing or attempting to induce a person to do any of the things referred to above;
31. being in any way, directly or indirectly, knowingly concerned in, or a party to, any of the things referred to above;
32. conspiring with others to do any of the things referred to above;
33. attempting to do any of the things referred to above.

4 Related Documents

- ANZCA Privacy Policy
- ANZCA Employee Code of Conduct
- ANZCA Information Security Policy
- ANZCA Electronic Communications Policy

5 Policy Review and Change Control

Version	Policy Owner	Approved by	Approval Date	Section Modified	Next Review Date
1.0	ED-CIO	ICTGC	Nov-2023	Created to replace the ANZCA ICT Code of Conduct dated Apr-2016	Nov-2026