RANZCO
THE LEADERS IN EYE CARE

The Royal Australian and New Zealand College of Ophthalmologists

IT Usage Policy

Approved by: Board

Next review: 4 December 2018

Approval date: 4 December 2015

The Royal Australian and New Zealand College of Ophthalmologists
ACN 000 644 404
94-98 Chalmers Street, Surry Hills NSW 2010
Phone: +61 2 9690 1001 Fax: +61 2 9690 1321
www.ranzco.edu

1. Purpose and scope

To carry out its objectives and business functions, RANZCO operates a complex IT Resource network across multiple infrastructure platforms. This policy outlines the standards of conduct; access rights; permissions; and repercussions for any person utilising RANZCO IT Resources.

This policy also sets out the type of surveillance that may be carried out in relation to use of RANZCO's IT Resources.

RANZCO IT Resources contain information that is of commercial and strategic value, personal in nature, and classified as sensitive material by the Privacy Act 1988 (Cth) (Australia) and Privacy Act 1993 (New Zealand). This policy is subject to, and does not supersede the RANZCO Privacy Policy and RANZCO Intellectual Property Policy.

This policy does not form part of any employees' contract of employment. Nor does it form part of any other person's contract for service.

2. Access to IT Resources

2.1 Lawful Use

The use of IT Resources must be lawful at all times. Unlawful use will breach this Policy and will be dealt with as a discipline offence.

Unlawful use of IT Resources may also lead to criminal or civil legal action being taken against individual authorised users. This could result in serious consequences such as a fine, damages and/or costs being awarded against the individual or even imprisonment.

RANZCO will not defend or support any authorised user who uses RANZCO IT resources for an unlawful purpose.

2.2 Granting of Access

Access to IT Resources is authorised by the relevant General Manager or Executive Officer, and provided by IT Staff. Access is normally based on a need to access that IT Resource, and an individual's current status and/or relationship with RANZCO.

2.3 User Declaration Form

Users may be required to complete a User Declaration form prior to authorisation being granted for access to certain IT Resources.

2.4 Intellectual Property (IP)

Ownership of existing or future IP which has been created or developed using the full or partial contribution or use of the resources of the College will be vested in RANZCO.

2.5 Access on contract expiry or authorised access period

Computer, software and network access will cease on expiration of contract or end-date.

2.6 Responsibilities

Regarding Use of RANZCO Computer Accounts

Each authorised user is responsible for:

- The unique computer and account which RANZCO has authorised. These devices and accounts are not transferable;
- Selecting and keeping a secure password for each of these accounts, including not sharing passwords and logging off after using a device; and
- Familiarising themselves with legislative requirements which impact on the use of IT Resources and acting accordingly.

RANZCO takes no responsibility for users whose actions breach policy, procedure or applicable legislation.

2.7 Restrictions to Access

Users are expressly forbidden unauthorised access to accounts, data or files on RANZCO IT Resources or any other IT resource. The Administrator of an IT Resource may restrict access to an individual user on the grounds that the user is in breach of this policy.

2.8 Third Party Access

Entities other than RANZCO may neither negotiate nor grant third parties access to RANZCO's communications and network infrastructure. Requests for access should be made in writing to RANZCO and approved by the relevant Manager and/or Executive Officer.

3. Personal Use of Information Technology Resources

3.1 Extent of Personal Use

A user who is authorised to use RANZCO's IT Resources may also use the IT Resources for limited, incidental personal purposes. Personal use of IT Resources is permitted provided such use is lawful, does not negatively impact upon the user's work performance, hinder the work of other users, adversely affect RANZCO's network, or damage the reputation, image or operations of RANZCO. Personal use must not cause noticeable additional cost to RANZCO.

3.2 Commercial Use

IT Resources must not be used for private commercial purposes except where RANZCO holds an interest and has authorised prior consent in writing.

3.3 Liability

RANZCO accepts no responsibility for:

- Loss or damage or consequential loss or damage, arising from personal use of the RANZCO's IT Resources.
- Loss of data or interference with regard to personal files and information arising from personal use of RANZCO's IT Resources.

4. Internet, Email and Messaging

4.1 Access to the Internet

4.1.1 Work Purposes

Authorised users are permitted to access the Internet for work related purposes.

4.1.2 Personal Usage

Authorised users are permitted access to the Internet (including WiFi) for personal purposes provided such use is lawful and reasonable in terms of time and cost to RANZCO.

Examples of permitted personal use are:

- Online banking
- Travel bookings
- Browsing

Examples of activities that are not permitted are:

- Streaming music, e.g. digital radio and/or sporting events
- Watching lengthy non work-related videos, i.e. in excess of 15 minutes
- Downloading large non work-related files

4.1.3 Guest Use

Guests are permitted to access the internet only on the guest network. Guests are permitted to access the internet over the RANZCO Guest network for Work purposes in which RANZCO holds and interest, and for Personal use.

4.2 Email, Messaging and Video Conferencing

4.2.1 User Responsibilities

When using RANZCO's Email, Messaging, Video Conferencing or any other communications system, users must at all times:

- Use RANZCO accounts for the sole use of RANZCO business activity;
- Respect the privacy and personal rights of others;
- Take all reasonable steps to ensure privacy, intellectual property and copyright is not infringed – refer section 4.2.3;
- Take all reasonable care not to plagiarise another person's work; or
- Not defame another person;
- Not forward or otherwise copy a personal email (except with permission of the author) or an email which contains personal information or an opinion about a person whose identity is apparent (except with permission of that person);
- Not send forged messages, or obtain or use someone else's e-mail address or password without proper authorisation;
- Not send mass distribution bulk messages and/or advertising without approval of the users General Manager;
- Not send SPAM. SPAM is defined by the *Spam Act (2003) (Commonwealth)*
- Not harass, intimidate or threaten another person/s – refer also to section 4.2.2;
- Not send sexually explicit material, even if it is believed that the receiver will not object. Remember, the intended receiver may not be the only person to access the communication – refer to section 4.2.2; and
- Adhere to the practices as set out in sections 4.2.2, 4.2.3 and 4.2.4 below.

4.2.2 Standards When Using IT Communication Resources

Appropriate civility should be observed when using e-mail and other communication services to communicate with staff, members, trainees or any other messaging recipients. When using any RANZCO email or communications system users must adhere to the guidelines set in the:

- RANZCO Anti-Discrimination and Equal Opportunity Policy
- RANZCO Discrimination, Harassment and Bullying Policy
- RANZCO Staff Code of Conduct
- RANZCO Privacy Policy

4.2.3 Forwarding of Emails – Privacy, Copyright and Intellectual Property

RANZCO owns all e-mail correspondence created by members of its staff in relation to their employment duties.

Care must be taken if an email contains personal information as defined by the RANZCO Privacy Policy. This kind of information must not be forwarded or copied without prior permission from the person who is the subject of the personal information.

Intellectual Property and Copyright in a personal/non-work related e-mail belongs to the writer of the message. A personal e-mail must never be copied or forwarded without permission of the writer.

4.2.4 Private Commercial Use

The private commercial use of e-mail, messaging or any other component of the RANZCO communications systems is not allowed. Communications must not be used for private commercial purposes except where RANZCO holds an interest.

5. Security of Information Technology Resources and Data

5.1 Authorised User's Responsibilities

Authorised Users have a responsibility at all times to:

- Act lawfully;
- Not compromise or attempt to compromise the security of any IT Resource belonging to RANZCO, any other organisation, or individual, nor exploit or attempt to exploit any security deficiency.
- Take reasonable steps to ensure physical protection including damage from improper use, food and drink spillage, electrical power management, anti-static measures, and protection from theft;
- Ensure their devices are not left unattended without first logging-out and/or securing the entrance to the work area – particularly if the system to which they are connected contains sensitive or valuable information; and
- Adhere to the practices as set out in sections 5.2, 5.3 and 5.4 below.

5.2 Records Management

Authorised Users are required at all times to:

- Take reasonable steps to ensure that important data is stored appropriately for preservation and backup;
- Observe appropriate RANZCO record management protocols.

5.3 Confidential Information

Authorised Users must at all times adhere to the RANZCO Privacy Policy and have a duty to keep confidential:

- All RANZCO data unless the information has been approved for external publication; and

- Information provided in confidence to RANZCO by other entities; and

Each staff member is under a duty not to disclose RANZCO business information unless authorised to do so. Breach of confidentiality through accidental or negligent disclosure may expose a User to disciplinary action.

5.4 Personal and Sensitive Information

Information about an individual, must not be disclosed without consent of the individual concerned except where explicitly stated in the RANZCO Privacy Policy.

5.5 RANZCO Liability

RANZCO accepts no responsibility for:

- Loss or damage or consequential loss or damage, arising from the use of RANZCO's IT Resources.
- Loss of personal data or interference with files arising from RANZCO's efforts to maintain IT Resources.

5.6 Bring your own Device (BYOD) Considerations

RANZCO grants employees, Fellows and other approved agents (collectively referred to as users) the privilege of using personal devices of their choosing for completion of works conducted for or on behalf of RANZCO. RANZCO reserves the right to revoke this privilege if users are found in breach of this or any other RANZCO policy.

This clause is intended to protect the security and integrity of RANZCO's data and technology infrastructure. Limited exceptions to this policy may occur due to variations in devices and platforms.

- Users may use their personal devices to access the following RANZCO services: email, calendars, contacts, intranet and extranet, OneDrive and Microsoft Dynamics CRM.
- Personal devices include but are not limited to personal computers, laptops, mobile telephones and tablets.
- RANZCO IT will assist with accounts and connectivity issues at RANZCOs offices only. Personal devices remain the responsibility of the owner, and any issues should be addressed with the manufacturer or telecommunications provider.
- In order to prevent unauthorised access, personal devices must be password protected using the features of the device and a strong password is required to access the RANZCO network or resources. It is the responsibility of users to select secure passwords and change them as necessary.
- The device must lock itself with a password, PIN or biometric means if it is idle for five minutes or longer.

- RANZCO reserves the right to disconnect the device from the network and remotely wipe any data stored if the device is lost, the user terminates his or her association with RANZCO, and/or RANZCO IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.
- RANZCO reserves the right to disconnect devices or disable services without notification.
- Any lost or stolen device must be reported to the company within 24 hours.
- Users are responsible for notifying their mobile carrier immediately upon loss of a mobile device if applicable under their carriers Terms.

6. Prohibited use of IT Resources and Possible Consequences

6.1 Business Activities

Authorised users are not permitted to run a business on RANZCO IT Resources for personal or professional gain.

6.2 Unauthorised Access

Authorised users are expressly forbidden from unauthorised access or attempting to gain unauthorised access to IT Resources belonging to other organisations.

6.3 Cause Damage

User are forbidden from willful or negligent cause of damage to RANZCO IT Resources, or personal devices connected to RANZCO's IT Resources. Actions that adversely affect the performance of RANZCO IT Resource are considered damaging even if performance is only temporarily affected.

6.4 Infringement of Intellectual Property and Copyright

Willful or negligent infringement of intellectual property or copyright may attract:

- Personal liability for damages;
- Denial of access to computer facilities; and
- Disciplinary action.

6.5 Software as a Service (SaaS) Applications

Use of SaaS applications provisioned by RANZCO are governed by individual user license agreements. Users are required to comply with use restrictions set out by the security settings and operational procedures and guidelines of the specific SaaS application, site or as stated in the license agreement.

6.6 Peer to Peer File Sharing

Installation or use of peer to peer file sharing software such as Kazaa, BitTorrent, etc. is not permitted on the RANZCO network. RANZCO provides alternative technologies for file sharing where appropriate.

6.7 Pornography and other Offensive Material

Authorised users are not permitted to utilise RANZCO IT Resources to access create, store or distribute pornographic material of any type or any other material of an obscene or offensive nature.

6.8 Gambling

Authorised users are not permitted to utilise RANZCO IT Resources to gamble.

6.9 Possible Consequences

6.9.1 For RANZCO Staff

Staff found to have breached this policy will be subject to disciplinary action in accordance with the RANZCO Performance and Misconduct policy, and may include, but is not limited to, any combination of:

- A warning of policy breach;
- Temporary or permanent suspension of access to RANZCO IT Resources;
- Temporary or permanent suspension of employment;
- Non-renewal of contractual arrangements; or
- Legal action.

Enforcement of disciplinary action is at the full discretion of RANZCO.

6.9.2 Authorised Users Other than RANZCO Staff

Authorised users (other than RANZCO staff) found to have breached this policy may be subject to appropriate action as determined by the College. Such action may include but is not limited to; removal of access to RANZCO IT Resources.

Criminal offences will be reported to the police.

7. Privacy and Surveillance

7.1 Security and Privacy

Accounts, software and data including, but not limited to, files and e-mail belonging to any user operating any device, not protected by law, over the RANZCO Network are subject to monitoring at RANZCO's discretion.

7.2 Access to and Monitoring

RANZCO reserves the right to access and monitor any computer or other electronic device connected to RANZCO Infrastructure, where not protected by law. This includes equipment owned by RANZCO and personal devices (e.g. laptops, tablets and mobile phones) that are connected to the network.

Access to and monitoring of equipment is at the sole discretion of RANZCO for any reason, including but not limited to, suspected breaches by the user of his/her duties as a staff member, unlawful activities or breaches of RANZCO Policy. Access to and monitoring includes, but is not limited to e-mail, web site browsing, server logs and electronic files.

Security camera footage may be viewed by police if requested.

RANZCO may keep a record of any monitoring or investigations.

7.3 Prior Approval Required

Prior approval must be obtained from the relevant General Manager or the User before a user's e-mail, files or data may be accessed by authorised staff.

8. Variations

RANZCO reserves the right to modify, replace or terminate this policy at any time.

9. References

Office of Parliamentary Counsel, (2003). *SPAM ACT 2003.* Canberra. Available at: http://www.austlii.edu.au/au/legis/cth/consol_act/sa200366/ [Accessed 04 December 2015].

10. Related Documents

- RANZCO Privacy Policy
- RANZCO Anti-Discrimination and Equal Opportunity Policy
- RANZCO Discrimination, Harassment and Bullying Policy
- RANZCO Staff Code of Conduct

11. Record of Amendments

Page	Details of amendment	Date approved