1. RACGP Information Technology Policy

1.1	Policy number:	IT-O-039.3
1.2	Category:	Organisational
1.3	Approval date:	September 2018
1.4	Revision date:	September 2019
1.5	Unit responsible	Office of the President and CEO

2. Policy declaration

This policy sets the standards of authorised RACGP usage of RACGP Technology Infrastructure. This policy must be read in conjunction with the RACGP Social Media Policy, Password Policy and Data Transmission Policy.

3. Definitions

In this Policy:

Confidential Information is information disclosed to a User or known to that User as a consequence of the User's engagement with the RACGP (including employees, contractors, volunteers, vendors, suppliers), and not generally known outside the RACGP, or is protected by law or which would be reasonably considered to be;

Information is defined as processed, stored or transmitted data. Information may constitute Confidential Information;

Technology Infrastructure includes all of the RACGP or User's devices (where access RACGP infrastructure), technology applications and platforms which are used by Users, at anytime and anywhere. It includes, all devices and any other means of accessing the RACGP's devices, technology applications and platforms;

Material includes, whether electronic or physical format, text, images, sound or any other material, sent either in an email or in an attachment to an email, or through a link to a site (URL) or in electronic message (for example an SMS) or as an attachment to a text message or in physical format; and

User includes any person who uses the Technology Infrastructure by any means.

Spam *includes* irrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc.

4. Scope

This policy applies to all Users.

5. General Information

5.1 Use of Technology Infrastructure

The Technology Infrastructure is provided to Users for RACGP purposes. The RACGP monitors all usage of the Technology Infrastructure as well as any and all materials, information and other content transmitted, received or stored in connection with this usage.

5.2 Operational Requirements

When using the Technology Infrastructure, Users must:

A. Use RACGP equipment in a responsible manner and keep secure;

B. Use their own username/login code and/or password for access to Technology Infrastructure and store their username/password confidentially and securely. Refer to the RACGP Password Policy;

C. Not permit third parties access to or control of RACGP data and Technology Infrastructure;

D. All devices, both RACGP and devices with access to RACGP data and Technology Infrastructure, are fully shut down when not in use, or protected by sufficient security measures such as a code to re-activate the device after being inactive. Devices must be locked when unattended to ensure no unauthorised access to your desktop device.;

E. Not interfere or attempt to interfere with any measures implemented by the RACGP;

F. Not remove the disclaimer automatically included in all RACGP emails as part of the signature block;

G. Not open an email, attachments, or click on hyperlinks that they suspect is spam, malicious, or contains a virus. Any security incident must immediately be reported to the RACGP Technology Operations Team;

H. Immediately notify their immediate manager or the relevant HR Officer of any Material breaching or which the User suspects breaches this policy, only delete the relevant content after reporting and confirming whether it is required for investigation, and not forward it to any other person;

I. Adhere to password requirements and policies including use of suitably complex passwords and changes to account passwords performed at regular intervals – refer to the *Password Policy*;

J. Not attempt to interfere with any antivirus or antimalware software installed as part of the RACGP Standard Operating Environment, enable any and all automatic updates to such software and not attempt to interfere with any regularly scheduled virus or malware scans;

K. Utilise suitable encryption software where sensitive data is transferred or when stored on a portable storage device, use of portable storage for sensitive data should be avoided where possible. Encryption software will be provided by the RACGP Technology Team;

L. Only install software on RACGP equipment or use any new device with prior written approval from the RACGP Technology Operations Manager or RACGP Digital Technology General Manager and which is supported by the RACGP Technology Team. All software authorised to be installed must be legally licensed by the RACGP.

5.3 Transmission, Storage and Retrieval of Confidential Information

Users may be in a position to transmit or receive sensitive and/or confidential data from time to time. Confidential information includes (but is not limited to):

A. Exam Content;

B. Exam Results;

C. Exam Details;

D. Customer Membership Details;

E. Financials (including credit card details);

F. Customer Experience;

G. Customer CPD Details;

H. Legal Correspondence;

I. Customer Contact Details;

J. Employee Salary;

K. Corporate Information;

L. Grants Information;

M. Copyright and Consent Forms;

N. Educational Activities;

O. Accounts Payable/Supplier Details;

P. Provider Details;

Q. Employee Contact Details; and

R. Recordings of Patient Consultations.

Users must adhere to advice received by the RACGP Technology Team for secure transmission and/or receipt of such data. This can include:

A. Use of RACGP approved encryption software to encrypt data prior to transmission, or transfer to a physical medium such as a USB drive;

B. Use of authorised media, either physical (for example USB drives) or electronic (for example streaming services) for transmission, storage and retrieval of Confidential Information.

C. Appropriate treatment of physical media and its secure disposal. This includes keeping all secure items in locked cabinets and sensitive information is disposed of using the secure disposal bins or secure media destruction services.

Please refer to the *Confidential Data Transmission Policy* document for more details.

5.4 Prohibited Conduct

Users must not use for any purpose or send (or cause to be sent), upload, download, use, retrieve, or access any Material on the Technology Infrastructure that:

A. Is prohibited by this Policy;

B. Breaches any applicable laws or regulations, promotes illegal activity or is fraudulent, or has the effect of being unlawful or fraudulent;

C. Is defamatory or libellous, obscene, violent, threatening, sexually explicit, indecent or of a pornographic nature, offensive, hateful or inflammatory;

D. Could adversely impact the image or reputation of an individual or the RACGP;

E. Will harass, upset, embarrass, alarm or annoy any other person or causes (or could cause) insult, offence, intimidation or humiliation or which lowers the reputation of a person or group of people;

F. Impersonates or misrepresents any other person;

G. Is misleading or deceptive or is likely to mislead or deceive;

H. Promotes discrimination of any kind;

I. Breaches the RACGP Social Media policy;

J. Could damage, disable, overburden or impair the Technology Infrastructure or interfere with any other party's productive use or enjoyment of the Technology Infrastructure;

K. Affects the performance of, or causes damage to the Technology Infrastructure in any way;

L. Knowingly transmits any data or material that contains viruses, Trojan horses, worms, time-bombs, keystroke loggers, spyware, adware or any other harmful programs or similar computer code designed to adversely affect the operation of any computer software or hardware;

M. Use any robot, spider, screen scraper, data aggregation tool or other automatic process to monitor, copy or extract any Information, or combine any Information with the information of a third party, without RACGP's prior written consent;

N. Reverse engineers, reverse assembles, decompiles or otherwise attempts to discover source code or other formulae or processes in respect of the Technology Infrastructure;

O. Transmit, or procure the sending of, any unsolicited or unauthorised advertising or promotional material or any other form of similar solicitation (otherwise known as spam); or

P. Gives the impression of or implies is representing, giving opinions or making statements on behalf of the RACGP without the RACGP's express authority.

Users must not use the Technology Infrastructure to:

A. Violate any third party's intellectual property rights, including by reproducing copyrighted documents or images;

B. Create or be responsible for the RACGP incurring any unauthorised legal obligation or liability;

C. Disclose any RACGP Confidential Information or information of any RACGP employee, member, client or supplier of RACGP without the RACGP's prior written consent;

D. Install software or run unknown or unapproved programs without receiving the prior written consent of the RACGP Technology Team;

E. Modify the software or hardware environments on Technology Infrastructure;

F. Gain unauthorised access into any other computer within or external to the RACGP, or attempt to deprive other Users of access to or use of the Technology Infrastructure;

G. Send or cause to be sent chain or spam emails or text messages in any format; or

H. Obtain personal gain, for example by running a personal business.

Unless authorised, Users must not interfere with, damage or disrupt:

A. Any part of the Technology Infrastructure;

B. Any equipment or network on which the Technology Infrastructure is stored;

C. Any software used for the Technology Infrastructure; or

D. Any equipment or network or software owned or used by any third party.

5.5 Details on blocking email and Internet Access

The RACGP will prevent (or cause to be prevented) the delivery of Material to or from a User, or a User's access to a website (including a social networking site), if the RACGP considers the relevant content breaches any of the provisions to clause 5

The RACGP will not give a prevented delivery notice for any email messages sent by a User if the RACGP is not aware (and could not reasonably be expected to be aware) of the identity of the User who sent the e-mail or is not aware that the e-mail was sent by the User.

5.6 Devices

Users wishing to access the Technology Infrastructure on a personal device must provide their manager's approval to the Technology Team and then provide that device to Technology

Team to ensure it is installed with appropriate software and/or configured appropriate to ensure the security and integrity of the Technology Infrastructure. Users must provide Technology Team will reasonable assistance to ensure the relevant software is installed.

Where requested, the User must promptly provide the RACGP with the relevant device (whether owned by the RACGP or the User) for the purpose of investigating any breach of this Policy.

Users must ensure portable devices that are used to access college information has an appropriate virus protection solution and security posture with up to date Operating System and Application patches installed and authentication protections to prevent unauthorised access to the device.

The RACGP reserves the right to require personal devices that are used to access RACGP information and/or systems to have installed specific software that allows the RACGP to remote wipe the device if lost, stolen or no longer employed.

Personal devices are supported where that device is supported by the RACGP.

6. Enforcement

Any breach of this policy may result in disciplinary action. This may include termination of employment (or, for persons other than employees, the termination or non-renewal of contractual arrangements).

Other disciplinary action that may be taken includes, but is not limited to, issuing a warning, suspension or disconnection of access to all or part of the Technology Infrastructure whether permanently or on a temporary basis.

For more serious issues, the RACGP may consult with relevant authorities.

7. Related policies, documents and legislation

A. Social Media Policy;

B. Privacy Policy:

C. Confidentiality Policy;

D. shareGP Policy;

E. employment Agreements;

F. RACGP updates to User’s from time to time;

G. Password Policy; and

H. Confidential Data Transmission Policy & Procedures

8. Administrative procedures

8.1 Access to published policy

This policy will be available via the RACGP intranet.

8.2 Review of this policy

This policy will be reviewed annually.