Mannum Medical Centre

Printed: 22/2/2019
Created: 01/06/2018
Last Revised: 29/10/2018
Review file: 1/5/2019

**PRINTED COPIES ARE NOT CONTROLLED**

### *Internet and Email Usage*

# Policy

All staff within the practice are to assist in mitigating security risks. This includes being aware of the risks associated with email and internet usage.

All staff are to use the internet, email and secure messaging in a manner which meet our privacy obligations and are to use such resources in a respectful and professional manner.

# Procedures

To avoid unnecessary risk to information systems, the following is advised:

**Internet usage**

- internet use for business, clinical and research purposes only
- all downloads accessed from the internet must be scanned for viruses
- all sites accessed must comply with legal and ethical standards
- web browser security settings are not to be changed without authorisation

In our practice, the type of firewall we have is recommended by our IT solutions provider and upgraded as necessary.

The firewall is tested on a monthly basis. The person responsible for testing the firewall is the Practice Manager and our IT provider Logic Plus .

This practice uses antivirus, anti-malware and anti-spyware which are centrally installed and managed and locally deployed.

**Email usage**

Communication with patients via electronic means (e.g. email) is conducted with appropriate regard to the privacy and confidentiality of the patient's health information.

Our practice uses the following confidentiality and privilege notice on outgoing emails that are affiliated with the practice:

**‘This message is confidential and should only be used by the intended addressee. If you were sent this email by mistake, please inform us by reply email and then destroy this message. The contents of this email are the opinions of the author and do not necessarily represent the views of the Mannum Medical Centre/Karoonda Medical Centre."**

Best practice when using email:

- Do not open unexpected email even from people known to you as this might have been spread by a virus.
- Use an antivirus mail filter to screen email before downloading.
- Save attachments and check for viruses before opening or executing them (note this does not relate to the clinical secure messaging but to attachments received through email and websites).
- Do not run programs directly from websites. If files are downloaded, check for viruses first.
- Email use that breaches ethical behaviours and/or violates copyright is prohibited.
- Do not send or forward unsolicited email messages, including the sending of ‘junk mail’ or other advertising material (email spam).

- Do not use email for broadcast messages on personal, political or non-business matters.
- Practice staff are never to send emails that might be construed as offensive or constitute as any form of harassment.

Emails and internet usage will be monitored by the Practice Manager including discretion to blacklist certain sites such as personal email or social media sites.

All staff have signed a computer use agreement as a condition of their employment.

**Useful Links**

**RACGP Social Media Guide** - http://www.racgp.org.au/your-practice/ehealth/social-media/guide/

**Recognise scam or hoax emails and websites** - https://www.staysmartonline.gov.au/your-identity/recognise-scam-or-hoax-emails-and-websites

**Australian Privacy Principles -** https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles