	WMC Wollondilly Medical Centre	**Printed: 20/06/2023** **Created: 02/06/2023** **Last Revised: 20/06/2023**

PRINTED COPIES ARE NOT CONTROLLED

Policy:

Electronic Communications Policy

Tahmoor & Wollondilly Centre both comply with the *Standards for General Practice* promulgated by the Royal Australian College of General Practitioners (as amended from time to time) in relation to information security and electronic communications (**Standards**).

In accordance with the Standards, the person who is designated as having primary responsibility for information security and electronic communications is the Practice Manager (Designated Practice Team Member). The Designated Practice Team Member's responsibilities include:

- knowing who and when to call for expert advice;
- giving relevant Practice employees the contact details of any external expert, the Practice has used;
- educating the Practice team about data security and the need to follow security protocols and policies; and
- monitoring whether employees are following security protocols and policies.

Email use

The Practice requires that electronic communication (e.g. via email) is conducted with appropriate regard to the private, confidential and sensitive nature of the health information with which the Practice deals. All employees must ensure that they use internet, email and secure messaging in connection with their work in a manner which complies with the Practice's privacy obligations, and in a respectful and professional manner.

The Practice uses the following confidentiality and privilege notice on outgoing emails that are affiliated with the Practice:

- IMPORTANT NOTICE : The information in this email is confidential. If you are not the intended recipient, any use or dissemination of the information and any disclosure or copying of this email is unauthorised and strictly prohibited. If you have received this email in error, please promptly inform us by reply email or telephone. You should also delete this email and destroy any hard copies produced. Please be aware any emails sent to the address listed will have standard level security protocols. If you have concerns involving sensitive health information, please make an appointment by phoning us on ##########

What constitutes best practice when using email?

When using email in connection with the Practice, all employees should be mindful to comply with the following practices:

- do not open an unexpected email, even from people known to you, without taking proper precautions
- use an antivirus mail filter to screen emails before downloading those emails;

- do not use the 'preview pane' in your email program as this automatically opens your email when you click on the header;
- 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 you need to download a file from a website, check for viruses first using antivirus software;
- do not send or forward unsolicited email messages, including the sending of 'junk mail' or other advertising material (ie email spam);
- do not use email for broadcast messages on personal, political or non-business matters.

Website safety and security

The Practice has a Service Level Agreement with Hawkhost for all web management services (**Agreement**). Andre Sarkis (owner) is responsible for liaising with Plumm Websites to ensure accuracy and currency of website content, compliance with [Guidelines for Advertising of Regulated Health Services](#) set by the Medical Board of Australia and management of the Agreement. Our website is hosted separately from Practice data.

Practice Specifics