Social Media Policy - Aiya Medical Centre

1. Social Media Use

1.1. Policy

'Social media' is defined as online social networks used to disseminate information through online interaction.

Regardless of whether social media is used for business related activity or for personal reasons, the following standards apply to members of our practice team, including general practitioners. Practitioners and team members are legally responsible for their postings online. Practitioners and team members may be subject to liability and disciplinary action including termination of employment or contract if their posts are found to be in breach of this policy.

1.2. Procedure

Our practice has appointed Krish as our social media officer with designated responsibility to manage and monitor the practice's social media accounts. All posts on the practice's social media websites must be approved by this person.

When using the practice's social media, all members of our practice team will not:

- Post any material that:
  - Is unlawful, threatening, defamatory, pornographic, inflammatory, menacing, or offensive.
  - Infringes or breaches another person's rights (including intellectual property rights) or privacy, or misuses the practice's or another person's confidential information (e.g. do not submit confidential information relating to our patients, personal information of staff, or information concerning the practice's business operations that have not been made public).
  - Is materially damaging or could be materially damaging to the practice's reputation or image, or another individual.
  - Is in breach of any of the practice's policies or procedures.
- Use social media to send unsolicited commercial electronic messages, or solicit other users to buy or sell products or services or donate money.
- Impersonate another person or entity (e.g. by pretending to be someone else or another practice employee or other participant when you submit a contribution to social media) or by using another's registration identifier without permission.
- Tamper with, hinder the operation of, or make unauthorised changes to the social media sites.
- Knowingly transmit any virus or other disabling feature to or via the practice's social media account, or use in any email to a third party, or the social media site.
- Attempt to do or permit another person to do any of these things:
  - Claim or imply that you are speaking on the practice's behalf, unless you are authorised to do so.
  - Disclose any information that is confidential or proprietary to the practice, or to any third party that has disclosed information to the practice.
- Be defamatory, harassing, or in violation of any other applicable law.
- Include confidential or copyrighted information (e.g. music, videos, text belonging to third parties).
- Violate any other applicable policy of the practice.

All members of our practice team must obtain the relevant approval from our social media officer prior to posting any public representation of the practice on social media websites. The practice reserves the right to remove any content at its own discretion.

Any social media must be monitored in accordance with the practice's current polices on the use of internet, email and computers.

Our practice complies with the Australian Health Practitioner Regulation Agency (AHPRA) national law, and takes reasonable steps to remove testimonials that advertise our services, which may include comments about the practitioners themselves. Our practice is not responsible for removing (or trying to have removed) unsolicited testimonials published on a website or in social media over which we do not have control.

Any social media posts by members of our practice team on their personal social media platforms should:

- Include the following disclaimer example in a reasonably prominent place if they are identifying themselves as an employee of the practice on any posting: '*The views expressed in this post are mine and do not reflect the views of the practice/business/committees/boards that I am a member of*'.
- Respect copyright, privacy, fair use, financial disclosure and other applicable laws when publishing on social media platforms.
- Avoid including any content that is defamatory, harassing or discriminatory in nature.

Social media activities internally and externally of the practice must be in line with this policy.

2. Email Use

2.1. Policy

Our practice is mindful that even if patients have provided electronic contact details, they may not be proficient in communicating via email and patient consent needs to be obtained before engaging in electronic communication via email. Communication with patients via email is conducted with appropriate regard to privacy.

2.2. Procedure

Whilst not encouraged, our practice allows patients an opportunity to obtain advice or information related to their care by email, but only where the general practitioner determines that a face-to-face consultation is unnecessary and that communication by email is suitable. Our practice will only provide information that is of a general, non-urgent nature and will not initiate email communication (other than SMS appointment reminders) with patients. Any email communication received from patients is also used as a method to verify the contact details we have recorded on file are correct and up-to-date.

Before obtaining and documenting the patient's consent, patients are fully informed through information contained in the practice's privacy policy of the risks associated with email communication in that the information could be intercepted or read by someone other than the intended recipient.

When an email message is sent or received in the course of a person's duties, that message is a business communication and therefore constitutes an official record. Patients are informed of any costs to be incurred as a result of the electronic advice or information being provided, and all electronic contact with patients is recorded in their health record.

All members of the practice team are made aware of our policy regarding email communication with patients during induction, and are reminded of this policy on an ongoing basis. They are made aware that email communications could be forwarded, intercepted, printed and stored by others. Each member of the practice team holds full accountability for emails sent in their name or held in their mailbox, and they are expected to utilise this communication tool in an acceptable manner. This includes, but is not limited to:

- Limiting the exchange of personal emails.
- Refraining from responding to unsolicited or unwanted emails.
- Deleting hoaxes or chain emails.
- Email attachments from unknown senders are not to be opened.
- Virus checking all email attachments.
- Maintaining appropriate language within electronic communications.
- Ensuring any personal opinions are clearly indicated as such.
- Confidential information (e.g. patient information) must be encrypted.

Our practice reserves the right to check an individual's email account as a precaution to fraud, viruses, workplace harassment or breaches of confidence by members of the practice team. Inappropriate use of the email facility will be fully investigated and may be grounds for dismissal.

The practice uses an email disclaimer notice on outgoing emails that are affiliated with the practice is as follows

WARNING: The information contained in this email may be confidential. If you are not the intended recipient, any use or copying of any part of this information is unauthorised. If you received this email in error, we apologise for any inconvenience and request that you notify the sender immediately and delete all copies of this email, together with any attachments. Any views expressed in this message are those of the individual sender, except where the sender specifically states them to be the views of Aiya Medical Centre.

3. Mobile Devices

3.1. Policy

For business and clinical purposes, some team members of Aiya Medical Centre are authorised to access practice software and emails via their personal mobile devices, including mobile telephones, laptops, tablets and hard drives. As these devices are at high risk of being lost, stolen or left unsecured, only certain team members are authorised to access data offsite.

Team members with this authorisation include the practice manager, who has access to emails for immediate notification of any urgent correspondence, and practice GPs, who can access patient health information through Best Practice in case of urgent results being delivered after hours. The Practice Manager, responsible for taking the backup hard drive offsite, also has authorisation to access practice information offsite on personal devices for the purposes of maintaining the backup data.

3.2. Procedure

Aiya Medical Centre monitors which devices can access practice data and which team members these devices belong to at all times, in case of breaches of privacy or termination of a team member's employment, which requires removal of access from personal devices.

Team Member Name and Role	Devices with Access	Access Type
Dr Ranjini Krishna, Principal Doctor	laptop	email access and access to Best Practice

When members of the practice team are granted authorisation, they are required to install appropriate password protection on all devices that can access practice information. Password protection should meet the requirements detailed in **Section 4 – Access Management.**

When practice team members use WiFi connection on mobile devices, they must ensure they adhere to the requirements detailed in **Section 3 – WiFi Usage**. If necessary, practice team members should request support from *IT Coordinator* to ensure that wireless connection has been set up securely.

Emails and clinical correspondence being sent by personal devices must meet the requirements of email communication detailed in **Section 7 – Electronic Transfer of Information.**

When mobile devices are not in use, practice team members must ensure that they store the devices securely to avoid damage or theft. Devices should all be kept in protective cases or laptop bags to avoid damage from bumping, dropping or other physical impacts. Devices are never to be left in high risk locations, such as within view on the seat of a locked car, or left unsupervised in a public place. In addition, when team members are working remotely they should ensure that they are positioned in a manner that information on their screens cannot be read by unauthorised persons. When working from home, a private, dedicated space is required for team members to perform their role with appropriate confidentiality.