EMAIL AND SOCIAL MEDIA POLICY

INTRODUCTION

This Practice uses email and social media platforms to share information with patients and members of the public about Federation Clinic (FCW) and our services, to promote FCW stories and news, to promote consumer engagement and support the delivery of high quality care.

DEFINITION

For the purposes of this policy, 'social media' includes online social networks used to disseminate information through online interaction.

PURPOSE

Regardless of whether email and/or social media is used for business-related activity or for personal reasons, the following policy requirements apply to all Practice users who are legally responsible for their online activities, and if found to be in breach of this policy disciplinary action may be taken.

COMMUNICATION VIA ELECTRONIC MEANS

Patients are able to obtain advice or information related to their care or appointment reminders by electronic means, where the doctor determines that a face-to-face consultation is unnecessary. Electronic communication includes: email, fax, and SMS. Patient consent is obtained prior to utilising the Practice SMS reminder and notification systems.

Practice staff and doctors determine how they communicate electronically with patients, both receiving and sending messages. All significant electronic contact with patients is recorded in the patient health records. Communication with patients via electronic means (e.g. email and Fax) is conducted with appropriate regard to the privacy Laws relating to health information and confidentiality of the patients health information.

Staff and Patients using email/SMS or other forms of electronic messaging should be aware that it is not possible to guarantee that electronic communications will be private. All personal health information or sensitive information sent by email must be securely encrypted. (Refer to section 6). Internal or external parties, including patients may send electronic messages. Messages from patients or those of clinical significance require a response to confirm receipt and should be documented in the patient medial record if clinically appropriate.

Employees should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed and stored by others. Staff members have full accountability for emails sent in their name or held in their mailbox, and 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 and reporting these to the Practice Manager
- Email attachments from unknown senders will not be opened
- Maintaining appropriate language within all e-communications

The Practice reserves the right to check individual emails as a precaution to fraud, viruses, workplace harassment or breaches of confidentiality by employees. Inappropriate use of the e-facilities will be fully investigated and may be grounds for dismissal.

Receiving and Responding to Email Communication

Patients, healthcare professionals and all other members of the public can make contact with the Practice via email. A quick & easy link is provided via our website.

Email addresses for public communication are:

- admin@federationclinic.com.au
- feedback@federationclinic.com.au

Both of the above email addresses are automatically forwarded to the Practice Manager for monitoring and management/reply in a timely manner. If the Practice Manager is absent, an out-of-office reply is set advising the sender of alternate contact options.

INDIVIDUAL STAFF EMAILS SHOULD NOT BE PROVIDED AS THESE ARE NOT MONITORED WHEN A STAFF MEMBER IS ABSENT.

Messages relevant to a patients clinical care should be copied and pasted into the patients files with associated notations of follow-up / reply.

Accessing the internet

The Internet is a vast computer network, comprised of individual networks and computers all around the world that communicate with each other to allow information sharing between users. It is important to adopt secure practices when accessing and using the Internet.

Staff members have full accountability for Internet sites accessed on their workstations, and are expected to utilise this tool in an acceptable manner including (but not limited to):

* Limiting personal use of the Internet
* Accessing only reputable sites and subject matter
* Verifying any information taken off the Internet for business purposes prior to use
* Not downloading any unnecessary or suspect information
* Being aware of any potential security risks - i.e. access / viruses and reporting to the Practice Manager
* Not disclosing any confidential information via the Internet without prior permission from the Practice Manager or Business Associates
* Maintaining the Practices confidentiality and business ethics in all dealings across the Internet
* Observing copyright restrictions relating to material accessed/downloaded.

PRACTICE SOCIAL MEDIA CONDUCT

The Practice's social media channels (if applicable) will be monitored on a regular basis. When using the Practice's social media, team members will not:

- Post any material that
    - is unlawful, threatening, defamatory, pornographic, inflammatory, menacing, offensive or in violation of any other applicable law.
    - infringes or breaches another person's rights or privacy, or misuses the Practice's or another person's confidential information, including copyrighted information (eg music, videos or text belonging to third parties)
    - 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 others to buy or sell products or services or donate money.
- impersonate another person or entity or by using another's registration identifier without permission.
- tamper with, hinder the operation of, or make unauthorized changes to the social media sites.
- knowingly transmit any virus or other disabling feature to or via the Practice's social media account.
- attempt to or permit another person to claim or imply that you are speaking on the Practice's behalf, unless authorised to do so.

PERSONAL SOCIAL MEDIA USE

Team members are free to personally engage in social media outside of work hours, as long as their actions do not have the potential to bring the Practice into disrepute. Team members may not represent their personal views expressed as those of this Practice.

- Any social media posts by staff on their personal social media platforms must no reveal confidential information about the Practice or a person who uses the Practice.
- If a team member identifies themselves on any social media platform as an employee of this Practice, their associated profile or relevant post must include a disclaimer indicating that the views they are expressing in that post are theirs and do not reflect the views of the Practice.
- When making public comment via social media, team members will not use an official work email address or provide other work contact information unless specifically authorised to do so.
- Staff must exercise discretion and use judgement when deciding to make public comment via social media platforms.