Donnybrook Family Doctors

Social Media Policy

Appropriate use of social media by DFD staff, contractors and representatives

Version	Effective date	Next review	Document owner
2.0	30 June 2026	30 June 2028	Practice Manager

RACGP Standards (5th ed): C3.5 Work health and safety · C6.4 Information security · C2.1 Patient feedback & complaints · AHPRA Advertising Guidelines and Code of Conduct · Privacy Act 1988 (Cth) and Australian Privacy Principles · applicable defamation, discrimination and consumer-protection law.

Approved by: Iminder Singh Nandha (Practice Manager) on behalf of Donnybrook Family Doctors Pty Ltd · Clinical Lead: Dr Nina Nandha (Practice Principal) · Applies to GPs, nurses, contractors, locums, students, reception/admin and any visiting clinicians.

1. Purpose

This policy sets out the requirements for appropriate use of social media by employees, contractors and representatives of Donnybrook Family Doctors.

It aims to protect patient confidentiality, maintain professional standards, comply with the RACGP Standards for general practices (5th edition), meet AHPRA advertising and professional conduct requirements and protect the reputation of the practice.

2. Scope

This policy applies to all employees (clinical and non-clinical), contractors, locums, students, volunteers and visiting clinicians at DFD.

It applies to both official practice social media accounts and personal accounts where an individual can be identified as associated with the practice.

3. Definition of social media

Social media includes platforms used to create, share or exchange content publicly or semi-publicly, including but not limited to:

- Facebook, Instagram, LinkedIn, TikTok, X (formerly Twitter), YouTube, Threads, Snapchat, Pinterest, Reddit
- Blogs, vlogs, podcasts and online forums
- Review platforms (Google Reviews, HotDoc reviews, Healthengine, Yelp, etc.)
- Messaging apps where content is shared with groups (WhatsApp groups, Telegram channels, Discord servers)

Email communication is governed primarily by the DFD Privacy Policy, Email, Internet & Electronic Communication Policy and Communication Policy.

4. Professional standards

- Where an individual can be identified as associated with DFD, communications must be professional, respectful and consistent with the AHPRA Code of Conduct.

- Staff must comply with the RACGP Standards, AHPRA obligations (including the Advertising Guidelines), the Privacy Act 1988 and applicable discrimination, defamation and consumer-protection laws.
- Views expressed in a personal capacity must clearly state they are personal and not those of the practice. A simple "Views my own" disclaimer on a profile does not override professional obligations.
- Staff must not make derogatory, discriminatory or unprofessional comments about patients, colleagues, other practices, partner organisations or community members on any platform.

5. Patient privacy and confidentiality

- Staff must not post patient information, identifiable or potentially identifiable, on any social media platform.
- Clinical images (photos, video, audio) must not be shared without written informed consent from the patient AND management approval.
- Clinical cases must not be discussed on social media, even if the practice considers the case de-identified — de-identification is harder than it looks, particularly in a small regional community like Donnybrook.
- Images and video taken within the practice must not include patients, clinical screens, medical records, computer monitors, appointment books, fridge contents or any identifiable third party.
- Staff must comply with the Privacy Act 1988 (Cth) and Australian Privacy Principles. Suspected breaches must be reported immediately under the DFD data breach process.

6. Professional boundaries

- Staff must not form personal social media relationships (e.g. "friend", "follow", direct messaging) with current patients.
- Clinical advice must not be provided via social media platforms — even in DMs or comments.
- All clinical communication must occur through approved practice systems (Best Practice, HotDoc secure messaging, MediSecure, official practice email).
- Where a patient initiates contact through social media, staff should redirect them to the practice telephone, online booking or appropriate clinical channel.

7. Official practice social media accounts

- Only staff authorised by the Practice Manager may create, access or post on behalf of DFD.
- All content must be reviewed and approved by the Practice Manager (or delegated authoriser) prior to publication.
- Content must be accurate, evidence-based and comply with AHPRA Advertising Guidelines for regulated health services.
- Account credentials are not shared via insecure channels; multi-factor authentication is enabled where available.
- Access is revoked promptly when a staff member's employment / contract ends or their role changes.

8. Advertising and testimonials

- The practice must not use testimonials relating to regulated health services in any advertising under the Health Practitioner Regulation National Law (s133) and AHPRA Advertising Guidelines.
- Content must not be misleading or deceptive, create unreasonable expectations or guarantee outcomes.
- Promotional content must be reviewed and approved by the Practice Manager prior to publication.
- Where a patient leaves an unsolicited positive review online, DFD must not republish or repost it as marketing.
- Use of "before and after" images for any procedure is not permitted without informed written consent and only where it complies with the AHPRA guidelines.

9. Online reviews

- Only authorised staff (Practice Manager or delegated authoriser) may respond to online reviews on behalf of DFD.
- Responses must not confirm whether an individual is or was a patient.
- Responses must not disclose any health, treatment or appointment information.
- Responses must remain polite, neutral and professional — even where the review is critical or factually inaccurate.
- Where a review contains a clinical concern, the patient should be invited offline to contact the practice directly (and the DFD complaints process applies).
- Defamatory reviews may be escalated to the platform's review process and, if necessary, to legal advice — never engaged with in public.

10. Personal use of social media

- Reasonable personal use of social media is permitted but must not disclose confidential information, identify patients, or damage the practice's reputation.
- Staff must comply with all applicable legislation including privacy, discrimination, defamation, work health and safety, and consumer-protection laws.
- Staff must not use practice-owned devices, accounts or wifi to access content that is illegal, offensive, sexually explicit or otherwise inappropriate for the workplace.
- Personal posts during working hours should be minimal and must not interfere with patient care or duties.

11. Incident management and breach reporting

- Any suspected breach of this policy, the Privacy Act or AHPRA obligations must be reported immediately to the Practice Manager.
- The Practice Manager will assess the suspected breach, including whether the Notifiable Data Breach Scheme applies, and coordinate the practice's response.
- Corrective actions may include taking down content, contacting affected patients, formal notification to the OAIC, AHPRA notifications, disciplinary action and a quality-improvement review.
- Incidents are recorded in the DFD incident register and reviewed under the practice's clinical governance process where clinical risk is involved.

12. Training and induction

- Staff receive social media policy training at induction and at least every two years thereafter.
- All new staff sign the DFD Computer Systems / Communications / Social Media Policy Acknowledgement as part of the onboarding pack.
- Periodic refreshers are run when AHPRA Advertising Guidelines, RACGP Standards or major platform terms change.

13. Disciplinary action

Failure to comply with this policy may result in disciplinary action, including formal warning, training requirement, restriction of access to practice systems, termination of employment or termination of any contractor / engagement agreement. Serious breaches may also be reported to AHPRA, the OAIC and any other relevant regulator.

14. Policy review

This policy is reviewed every two years or earlier if AHPRA, RACGP, OAIC, platform-specific or legislative changes occur. The next scheduled review is 30 June 2028.

15. Acknowledgement

By signing below, the staff member, contractor or visiting clinician acknowledges that they have read, understood and undertake to comply with this Social Media Policy.

Signatory	Name	Signature	Date
Staff / contractor / visiting clinician			
Approver — Practice Manager	Iminder Singh Nandha		

Filing & review: This Social Media Policy is held by the Practice Manager and reviewed every two years, or earlier after any material change to AHPRA Advertising Guidelines, RACGP Standards, the Privacy Act or major platform terms. Signed staff acknowledgements are filed in each person's profile folder in the DFD Accreditation Hub.