Donnybrook Family Doctors Communication Policy

Donnybrook Family Doctors

Communication Policy

Practice name: Donnybrook Family Doctors

Address: 92 South Western Highway, Donnybrook WA 6239

Phone: (08) 9731 1888

Fax: (08) 9731 1889

Email: info@dfdoctors.com.au

Website: www.donnybrookfamilydoctors.com.au

Document owner: Iminder Nandha, Practice Manager

Approved by: Dr. Nina Nandha, Practice Principal

Version: 1.0

Effective date: 05 / 04 / 2026

Review date: 05 / 04 / 2027

Review frequency: Annually, or sooner if systems, legislation, communication channels or RACGP Standards change

This policy is intended for internal practice use and supports safe, timely, respectful and privacy-compliant communication with patients, carers, other healthcare providers and external organisations.

1. Purpose

The purpose of this policy is to ensure that Donnybrook Family Doctors manages communication safely, respectfully, consistently and in accordance with privacy, confidentiality and accreditation requirements.

This policy sets out how the practice manages telephone, email, SMS, secure electronic messaging, voicemail, online bookings, telehealth and other communication channels. It also explains the practice requirements for patient consent, patient identification, message documentation, urgent communication and escalation.

2. Scope

This policy applies to all doctors, GP registrars, nurses, allied health practitioners, reception and administration staff, the Practice Manager, students, contractors and any other person who handles patient or practice information on behalf of Donnybrook Family Doctors.

It applies to communication with:

- Patients, prospective patients, parents, guardians, carers, substitute decision-makers and support persons
- External healthcare providers, hospitals, pathology providers, imaging providers, pharmacies and allied health providers
- Insurers, government agencies, legal representatives and other third parties
- Practice team members and clinical software users
- The public through the practice website, online booking platforms and social media channels

3. RACGP and Legal Alignment

This policy supports the practice to meet the current RACGP Standards for general practices applicable to the practice accreditation cycle, including the following areas:

- C1.2 — managing communications from patients, including telephone and electronic communication
- C1.3 — supporting informed patient decisions through clear and understandable communication
- C1.4 — interpreter and other communication services
- C6.1 — patient identification using a minimum of three approved patient identifiers
- C6.3 — confidentiality and privacy of health and other information
- C7.1 — content and accuracy of patient health records
- GP2.2 — follow-up systems for results, recalls and reminders
- C8.1 — education and training of non-clinical staff in their role and responsibilities

This policy also supports compliance with the Privacy Act 1988 (Cth), the Australian Privacy Principles, the My Health Records Act 2012 (Cth), applicable Western Australian legal requirements and the practice Privacy Policy.

4. Policy Statement

Donnybrook Family Doctors is committed to communication that is safe, timely, patient-centred, confidential and documented. All communication must protect patient privacy, use appropriate patient identifiers, be managed according to clinical urgency and be recorded in the patient health record when clinically relevant.

Patients must be informed of the limitations and risks of electronic communication. Urgent medical concerns must not be managed solely by email, SMS, website forms, social media or voicemail.

5. Responsibilities

Practice Principal: Approves this policy, oversees clinical governance and supports safe communication systems.

Practice Manager: Maintains this policy, trains staff, audits compliance, manages website/online information accuracy and coordinates privacy or communication incidents.

Doctors and GP Registrars: Provide clinical advice, review clinical messages, manage urgent and significant results, document clinical communication and determine what information can be safely communicated electronically.

Practice Nurses: Assist with triage and recalls within scope, document communication, escalate concerns to a doctor and verify patient identity before discussing clinical information.

Reception and Administration Staff: Manage appointments, incoming calls, messages, emails and SMS according to this policy; ask about emergencies before placing callers on hold; verify patient identity; and avoid giving clinical advice.

All Team Members: Maintain confidentiality, use approved communication systems only, report communication incidents and complete required privacy/communication training.

6. General Communication Principles

- Communication must be respectful, culturally safe, plain-language and appropriate to the patient's needs and health literacy.
- Patients must be given access to interpreter, National Relay Service, support person, carer or other communication assistance where required.
- Privacy and confidentiality must be maintained in all communication, including at reception, by phone, by email, by SMS and during telehealth.
- Clinical advice is provided only by appropriately qualified clinical team members.
- Reception staff may ask questions to determine appointment type and urgency, but must not provide clinical advice.
- Urgent and emergency matters must be escalated promptly and must not wait for routine message processing.
- Where communication relates to clinical care, recalls, results, referrals, medication, symptoms or patient safety, it must be documented in the patient health record.
- Only approved practice systems may be used for patient communication. Personal email accounts, personal messaging apps and personal devices must not be used to send identifiable patient health information unless specifically authorised under a documented emergency contingency process.

7. Patient Identification

The practice uses a minimum of three approved patient identifiers to correctly identify patients and their clinical information. Staff must ask the patient to state the identifiers. Staff must not read out patient details and ask the patient simply to confirm them, except where the patient has communication limitations and an alternative safe process is required.

7.1 Approved Patient Identifiers

- Family name and given names (together count as one identifier)
- Date of birth
- Gender as identified by the patient
- Current residential address
- Patient health record number, where it exists
- Individual Healthcare Identifier (IHI)

A Medicare number is not an approved RACGP patient identifier and must not be relied on as one of the three approved identifiers. It may still be collected or checked for billing or Medicare claiming purposes.

7.2 When Identifiers Must Be Used

- When a patient makes, changes or cancels an appointment
- When a patient presents to reception
- Before discussing health information by telephone, email or SMS
- Before giving test-result information or arranging recall appointments
- When a patient requests a prescription, referral, certificate, form, copy of results or transfer of records
- Before a telehealth or video consultation proceeds
- Before accessing or updating a patient health record
- When scanning, filing or attaching documents to a patient record
- When sending or receiving information about the patient to or from external providers

If the communication involves an emergency, staff must not delay emergency care in order to complete routine identification. Patient identity must be confirmed as soon as safe and practicable.

8. Consent for Communication

8.1 Recording Communication Preferences

Patient communication preferences must be recorded and kept current in the practice clinical or administrative system. This includes preferred phone number, email address,

SMS consent, permission to leave voicemail, preferred contact method and any communication assistance needs.

Patients are asked to notify the practice of changes to their name, address, phone number, email address, emergency contact, Medicare or concession details.

8.2 Consent for SMS and Email

- Patients may consent to receive appointment reminders, recalls, reminders, administrative information and selected healthcare-related messages by SMS or email.
- Patients must be informed that SMS and standard email may not be fully secure and may be seen by someone other than the intended recipient.
- Consent to communicate electronically must be documented in the patient record or registration record. If a patient initiates contact electronically, consent may be implied for responding to that particular communication, provided the response is appropriate and low risk.
- Patients may opt out of non-essential SMS or email communication at any time. Clinical safety communication, such as urgent recalls or significant results, may still require contact by the safest available method.
- Specific written consent is required before sending sensitive health information to a third party unless disclosure is required or authorised by law, necessary for healthcare, or otherwise permitted under the Privacy Policy.

8.3 Parents, Guardians, Carers and Substitute Decision-Makers

Information may be communicated to a parent, guardian, carer, substitute decision-maker or responsible person where the patient has consented, where the person has legal authority, where disclosure is necessary for healthcare and the patient cannot consent or communicate consent, or where disclosure is required or authorised by law.

For young people, clinicians assess confidentiality, capacity and parental access on a case-by-case basis. Mature minors may be able to consent to their own care and control access to their information depending on understanding and circumstances.

9. Telephone Communication

9.1 Incoming Calls

- Reception staff must answer calls courteously and identify the practice.
- Before placing a caller on hold, staff must ask whether the matter is an emergency or urgent medical concern.
- If the caller describes a life-threatening emergency or serious symptoms, staff must advise the caller to phone 000 immediately or attend the nearest Emergency Department. Staff may also alert a nurse or doctor where the caller is on site or the situation requires immediate practice action.

- Reception staff may ask questions to determine urgency, appointment type and appropriate booking length.
- Reception staff must not provide clinical advice. Clinical questions must be directed to a nurse or doctor, or the patient must be offered an appropriate appointment.
- Calls about chest pain, severe shortness of breath, stroke symptoms, collapse, severe bleeding, severe allergic reaction, sudden confusion or other red-flag symptoms must be escalated immediately.

9.2 Outgoing Calls

- The staff member must verify at least three approved patient identifiers before discussing health information.
- When leaving a message with another person or voicemail, only minimal information is to be provided unless the patient has consented to detailed messages.
- Standard wording should be used, such as: “This is Donnybrook Family Doctors calling for [first name]. Please contact the practice on (08) 9731 1888.”
- Detailed test results, diagnoses, medication information or sensitive matters must not be left on voicemail unless specifically authorised by the patient and clinically appropriate.
- All clinically relevant outgoing calls and outcomes must be documented in the patient record.

9.3 Telephone Messages for Doctors or Nurses

Messages for clinical team members must be entered into the approved practice message/task system or clinical record. Paper notes, sticky notes or informal verbal-only messages are not acceptable for clinical matters except during immediate emergencies, after which the details must be documented.

At a minimum, the message must include the date/time, caller name and relationship to patient, patient identifiers used, contact number, reason for call, urgency, staff member taking the message, action requested, responsible clinician/team member and outcome.

10. Email Communication

10.1 General Email Rules

- The practice email address is info@dfdoctors.com.au. Email is not suitable for emergencies or urgent medical concerns.
- The practice aims to respond to non-urgent emails within two business days. This timeframe may vary depending on workload, public holidays and clinical priorities.
- Patients are informed that email may not be monitored continuously and should call the practice for urgent matters or call 000 in an emergency.
- Clinical advice by email is only provided where a doctor or nurse determines that it is clinically appropriate and safe.

- Incoming emails containing clinical information must be reviewed, triaged, imported or documented in the patient record and allocated to the appropriate team member.
- Email correspondence must not be deleted if it forms part of the clinical or administrative record.

10.2 Sending Health Information by Email

- Secure electronic messaging is preferred for clinical communication with other healthcare providers.
- Health information may be sent by email only where clinically appropriate, privacy risks have been considered, the recipient details have been checked, and patient consent has been obtained or can be reasonably implied for the specific interaction.
- Before sending health information by email, staff must check the recipient email address, attachments, patient identity and content of the email.
- Only the minimum necessary information should be included.
- Subject lines should avoid sensitive clinical detail wherever possible.
- Sensitive documents should be sent using a secure method where available, such as secure messaging, password-protected file, encrypted system or approved portal.
- The email and any attachments sent or received must be saved, scanned or noted in the patient record where clinically relevant.
- Email must not be used as the sole method for urgent, serious, abnormal or life-threatening results unless specifically directed by a clinician and supported by additional contact attempts.

10.3 Email from Third Parties

Requests for patient information from insurers, lawyers, employers, schools or other third parties must not be actioned without appropriate patient consent or legal authority. Staff must escalate these requests to the Practice Manager or a doctor before disclosure.

11. SMS Communication

The practice may use SMS for appointment reminders, recalls, reminders, preventive health messages, administrative updates and selected healthcare-related communication. SMS communication is used in a way that minimises privacy risk.

- SMS messages must be brief and should not include detailed diagnoses, highly sensitive results or unnecessary clinical detail.
- Patients must be informed that SMS is not fully secure and may be viewed by someone other than the patient.
- Patients may opt out of non-essential SMS messages.
- Bulk SMS messages must be approved by the Practice Manager or authorised delegate and checked for accuracy before sending.

- SMS can be used as part of a recall or reminder process but must not replace clinician-directed urgent follow-up for clinically significant or high-risk results.
- Clinically relevant SMS communication and delivery/response outcomes must be recorded or retrievable in the patient record or approved communication system.

12. Secure Messaging and External Provider Communication

Secure electronic messaging, such as HealthLink or other approved secure messaging systems, is the preferred method for transferring clinical information between healthcare providers where available.

- Provider details must be checked before sending referrals, letters, results or clinical information.
- Clinical documents must be reviewed by the responsible clinician before being sent, especially where templates or automated document generation are used.
- Only information relevant to the purpose of the communication should be included.
- Incoming correspondence must be matched to the correct patient using approved identifiers, reviewed by the appropriate clinician and filed into the correct record.
- Failed transmissions or rejected secure messages must be followed up and documented.

13. Telehealth and Video Consultations

- Patients must be identified using at least three approved patient identifiers at the start of a telehealth or video consultation.
- The clinician should confirm the patient's current location and a contact number at the start of the consultation where clinically appropriate, especially for urgent or higher-risk presentations.
- The clinician must assess whether telehealth is clinically appropriate. If a physical examination, procedure, test, vaccination or urgent assessment is required, the patient must be advised to attend in person or seek emergency care.
- Patients should be encouraged to participate from a private location where possible.
- Audio or video recording of a consultation must not occur without the knowledge and consent of all relevant parties. Any clinically required image, recording or screenshot must be managed as part of the patient health record.
- Telehealth notes must be documented in the patient record in the same way as face-to-face consultations.

14. Online Bookings, Website and Social Media

- Online booking platforms may be used for appointment booking and administrative information. They must not be used for emergency care.
- The practice website and online booking information must be kept current, including phone number, opening hours, emergency instructions, after-hours care, fees and communication limitations.

- The Practice Manager or delegated staff member is responsible for coordinating updates to website, HotDoc, Google Business Profile, Healthdirect, voicemail and reception signage.
- Social media must not be used for individual clinical advice, test results, medication requests, complaints involving personal health information or urgent medical concerns.
- Any patient information received through website forms or social media must be handled confidentially, documented where clinically relevant and redirected to an appropriate communication channel.

15. Communication Requiring Urgent Escalation

Any communication suggesting serious illness, immediate risk, patient safety concern or clinically significant deterioration must be escalated promptly to a nurse, doctor or emergency service as appropriate.

Examples include:

- Chest pain, severe shortness of breath or suspected stroke symptoms
- Collapse, loss of consciousness, severe bleeding or severe allergic reaction
- Severe abdominal pain, acute neurological symptoms or sudden confusion
- Suicidal thoughts, risk of harm to self or others, domestic/family violence safety concerns
- High-risk, seriously abnormal or life-threatening pathology or imaging results
- Post-procedure complications or serious medication reactions

Staff must document urgent communications, escalation steps, advice given, contact attempts and final outcome. If emergency services are advised, this must be recorded.

16. Results, Recalls and Reminders Communication

The practice maintains systems to follow up investigation results, recalls and reminders. Communication about results and recalls must be managed according to clinical significance and documented in the patient record.

- Clinically significant results are reviewed by a doctor and actioned according to clinical urgency.
- High-risk or life-threatening results require immediate escalation according to the Results and Recall Policy or Health Information Management Policy.
- SMS, email or letter may be used for routine reminders and non-urgent recalls where appropriate and consented.
- Significant or urgent results must not rely solely on passive communication or a single SMS/email unless specifically authorised by the responsible clinician and supported by documented follow-up.

- Contact attempts must be documented, including date, method, staff member, outcome and further action.
- Patients are advised that no news does not always mean normal results and should contact the practice if they have not received expected results.

17. Message Documentation Requirements

The following communication must be documented in the patient health record or approved practice system when clinically relevant:

- Phone calls about symptoms, clinical advice, results, recalls, referrals, medication, forms or urgent concerns
- Emails or SMS messages containing clinical information or patient safety information
- Voicemail messages left or received where they relate to patient care
- Contact attempts for recalls, reminders, urgent results, missed appointments of clinical concern or follow-up care
- Communication with carers, family members, guardians, substitute decision-makers or third parties
- Referrals, handovers, clinical correspondence and secure messaging activity
- Patient consent or refusal for electronic communication or disclosure to another person

17.1 Minimum Documentation Standard

Date and time: Date/time of call, email, SMS, voicemail or message

Identity: Three identifiers used, or reason an alternative process was required

Person communicating: Patient, parent, carer, guardian, external provider or staff member

Issue/request: Brief summary of the matter, symptoms, result, request or concern

Risk/urgency: Routine, urgent, emergency/red flag, clinically significant result, etc.

Advice/action: Advice given, appointment booked, message sent to GP, 000 advised, recall created, etc.

Responsible person: Doctor, nurse, staff member or team allocated to follow up

Outcome: Spoke with patient, left voicemail, SMS sent, email received, unable to contact, recall closed, etc.

18. Internal Communication and Handover

- Clinical messages and tasks must be communicated using the approved clinical software/task system wherever possible.

- Urgent matters must be verbally escalated to an appropriate clinician in addition to electronic documentation.
- Staff must avoid discussing patient information where conversations can be overheard by other patients or unauthorised persons.
- Printed lists, notes and correspondence containing patient information must be secured and disposed of confidentially when no longer required.
- Handover between team members must include enough information to maintain patient safety without sharing unnecessary information.

19. Privacy, Confidentiality and Minimum Necessary Disclosure

All communication must comply with the practice Privacy Policy and Health Information Management Policy. Information is disclosed only with patient consent, where necessary for healthcare, where required or authorised by law, where necessary to prevent or lessen a serious threat to health or safety, or where otherwise permitted under privacy legislation.

- Only the minimum necessary patient information should be communicated for the purpose.
- Staff must check recipient details before sending information.
- Staff must not disclose whether a person is a patient of the practice unless authorised or necessary for healthcare or safety.
- Communication errors, misdirected emails/SMS/faxes, wrong-patient documentation or suspected privacy breaches must be reported to the Practice Manager as soon as possible.
- The Practice Manager will coordinate breach assessment, containment, documentation and notification where required.

20. Interpreter, Accessibility and Communication Support

The practice supports patients to communicate effectively and safely. Patients should be asked whether they need an interpreter, National Relay Service, Auslan, a support person, plain-language explanation or other communication assistance.

- Interpreter or communication assistance needs must be recorded in the patient record.
- Patients should be encouraged to request interpreter support when booking appointments.
- Family members may assist where appropriate, but professional interpreters should be used for complex, sensitive or high-risk clinical communication where possible.
- Communication must be adapted for patients with hearing, vision, cognitive, mobility, language or literacy needs.

21. Staff Training and Monitoring

- All new staff receive induction on this policy, privacy, confidentiality, patient identification, emergency escalation and message documentation.
- Non-clinical staff receive training appropriate to their role, including not providing clinical advice and escalating urgent concerns.
- Staff training is documented in the practice training register.
- The Practice Manager may conduct audits of message documentation, identifier use, recall contact attempts, email/SMS consent and website/online information accuracy.
- Communication incidents and near misses are reviewed for quality improvement.

22. Communication Incidents and Breach Management

A communication incident includes any event where communication may have caused or could have caused patient harm, privacy breach, delay in care, wrong-patient information, missed message, lost result, misdirected correspondence or inappropriate disclosure.

Examples include:

- Email, SMS, fax or letter sent to the wrong recipient
- Message not passed to the responsible clinician
- Urgent communication not escalated promptly
- Test result or recall not followed up according to policy
- Patient information discussed where it could be overheard
- Communication made without appropriate consent or authority

Incidents must be reported to the Practice Manager or Practice Principal. The practice will contain the incident, assess risk, notify affected parties where required, document actions taken and implement quality improvement measures.

23. Related Documents

- Donnybrook Family Doctors Privacy Policy
- Donnybrook Family Doctors Health Information Management Policy
- Results, Recalls and Reminders Policy
- New Patient Registration Form and consent forms
- Email and SMS consent documentation
- Complaints and Feedback Policy
- Data Breach Response Procedure
- Staff Induction and Training Register
- Social Media and Website Procedure, where applicable

24. References and Guidance

- RACGP Standards for general practices — current edition applicable to the practice accreditation cycle
- RACGP Criterion C1.2 — Communications
- RACGP Criterion C6.1 — Patient identification
- RACGP Criterion C6.3 — Confidentiality and privacy of health and other information
- RACGP Criterion GP2.2 — Follow-up systems
- RACGP information security guidance on electronic sharing of information and using email in general practice
- Privacy Act 1988 (Cth) and Australian Privacy Principles
- Office of the Australian Information Commissioner — Guide to health privacy and Notifiable Data Breaches scheme

25. Document Control

Version: 1.0

Effective date: 05 / 04 / 2026

Review date: 05 / 04 / 2027

Changes made: New RACGP-aligned Communication Policy

Approved by: Dr. Nina Nandha, Practice Principal

Next review: 05 / 04 / 2027 (annual, or sooner if practice details, legislation or RACGP Standards change)

Appendix A — Quick Guide: Communication Channel Rules

Phone

Suitable for: Appointments, urgent triage, results contact, recalls, patient queries

Not suitable for: Leaving detailed sensitive information on voicemail without consent

Documentation: Document clinical calls and outcomes

Email

Suitable for: Non-urgent administrative matters, selected documents with consent, external provider communication where secure messaging not available

Not suitable for: Emergencies, urgent symptoms, high-risk results as sole method

Documentation: Save or note clinically relevant email in record

SMS

Suitable for: Appointment reminders, routine recalls/reminders, brief administrative messages

Not suitable for: Detailed sensitive information, urgent/high-risk results as sole method

Documentation: Retain delivery/response records where relevant

Secure messaging

Suitable for: Clinical letters, referrals, reports to/from healthcare providers

Not suitable for: Consumer messaging unless designed/approved for that purpose

Documentation: File incoming/outgoing correspondence

Voicemail

Suitable for: Request for patient to call the practice

Not suitable for: Detailed results/diagnoses unless specifically consented and clinically appropriate

Documentation: Document clinically relevant voicemail

Social media

Suitable for: General public information approved by practice

Not suitable for: Clinical advice, results, urgent matters, complaints with PHI

Documentation: Redirect to appropriate channel

Appendix B — Reception Prompt for Incoming Calls

Suggested prompt:

"Good morning/afternoon, Donnybrook Family Doctors. Before I place you on hold or take your details, is this an emergency or urgent medical concern?"

If yes or uncertain:

- Ask brief safety questions only to determine urgency and location, not to provide clinical advice.
- For life-threatening symptoms, advise the caller to call 000 immediately.
- Escalate to nurse/doctor according to availability and practice procedure.
- Document the call and action taken.

Appendix C — Patient Identifier Prompt

Suggested wording:

"For privacy and safety, I need to confirm three details. Can you please tell me your full name, date of birth and current address?"

Alternative identifiers may be used where appropriate, including gender as identified by the patient, patient health record number or IHI. Medicare number is not used as an RACGP-approved identifier.

Appendix D — Minimum Message Note Template

Use the following structure when documenting clinically relevant communication:

- Date/time:
- Communication method: phone / voicemail / email / SMS / secure message / in person / telehealth
- Person communicating and relationship to patient:
- Patient identifiers confirmed:
- Reason for contact:
- Urgency/risk level:
- Information/advice provided:
- Action taken:
- Responsible clinician/team member:
- Follow-up required and due date:
- Outcome/contact attempts: