Donnybrook Family Doctors

Email, Internet and Electronic Communication Policy

Document title	Email, Internet and Electronic Communication Policy
Practice	Donnybrook Family Doctors
Version	2.0
Effective date	03 June 2026
Next review date	03 June 2027
Policy owner	Practice Manager
Approved by	Iminder Nandha
Replaces	Email & Internet Policy, effective 30 May 2023
Relevant accreditation area	RACGP Standards for general practices, 5th edition — Criterion C6.4 Information security

Policy statement

Donnybrook Family Doctors uses email, internet services and other electronic communication systems to support safe, efficient healthcare delivery. Staff must use these systems lawfully, professionally and securely, with particular care when handling patient health information and other confidential information.

1. Purpose

This policy sets out the requirements for acceptable, secure and professional use of email, internet services and electronic communication systems at Donnybrook Family Doctors.

The purpose of this policy is to:

- support safe communication with patients, health providers, suppliers and other approved parties;
- protect patient privacy and confidentiality;
- reduce the risk of unauthorised access, misuse, loss or disclosure of personal and health information;
- support compliance with the Privacy Act 1988, Australian Privacy Principles and RACGP Standards;
- provide staff with practical rules for email, internet, attachments, phishing, remote access and personal use.

2. Scope

This policy applies to all employees, GPs, registrars, contractors, locums, students, volunteers and other authorised users who access practice email, internet services, clinical software, administrative systems, practice-owned devices or practice information.

It applies when accessing practice systems from the clinic, from home, remotely, on mobile devices, or through any approved cloud-based service.

3. Key obligations and source documents

Requirement area	How this policy addresses it
RACGP Standards C6.4	The practice must maintain an email policy, ensure staff understand email / social media risks, maintain secure passwords, verify email addresses, inform patients of privacy risks, and obtain consent where email is used.
RACGP email guidance	Unencrypted or unsecured email can create privacy and security risks. Practices should assess risk, verify email addresses, obtain and record consent, and use password protection, encryption or secure websites where appropriate.
RACGP electronic sharing guidance	Clinical information should preferably be sent using secure electronic messaging from within clinical software where available.
Privacy Act / Australian Privacy Principles	The practice must take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure.
Practice policies	This policy must be read with the Privacy Policy, Health Information Management Policy, Communication Policy, Social Media Policy, Data Breach / Cyber Incident Procedure and Computer System / Password Policy.

4. Definitions

Term	Meaning
Email	Messages sent or received using practice email accounts, clinical software email functions or other approved practice systems.
Internet services	Websites, web-based applications, cloud services, search engines, portals and online forms used for practice work.
Electronic communication	Email, SMS, online forms, portals, secure messaging, web-based

Term	Meaning
	correspondence and other digital communication tools.
Patient health information	Any information or opinion about a patient's health, healthcare, appointment, Medicare details, test results, referrals, prescriptions or identity in a health context.
Secure messaging	Approved secure electronic messaging used to send clinical information between healthcare providers, usually from within clinical software.
Confidential information	Patient information, business information, staff information, login details, financial information, contracts and any information not intended for public release.

5. Roles and responsibilities

Role	Responsibility
Practice Principal / Clinical Lead	Provides clinical governance for patient communication, privacy, disclosure of clinical information and incident response.
Practice Manager	Owns this policy, maintains staff acknowledgements and training evidence, manages breaches, audits compliance and updates procedures.
Computer Security / IT Lead	Oversees account security, MFA, device security, remote access, backups, antivirus / firewall arrangements and liaison with IT support.
Doctors and clinical staff	Use secure channels for clinical information, verify recipients, document patient communication, and escalate privacy or safety concerns.
Reception / admin staff	Follow approved procedures for patient emails, identity checks, attachments, online forms, appointment information and escalation.
All users	Keep passwords secure, report suspicious emails, avoid unauthorised disclosure, lock screens and comply with this policy.

6. Acceptable use of email and internet

Practice email and internet access are provided primarily for work and work-related purposes. Acceptable use includes:

- communicating with patients, healthcare providers, suppliers, insurers, government agencies and other approved parties for legitimate practice purposes;
- accessing approved clinical, administrative, training, accreditation, billing and regulatory resources;
- communicating about appointments, recalls, referrals, results, requests and other practice business in accordance with approved procedures;
- limited personal use where it is brief, infrequent, lawful, does not interfere with work duties, does not create cost or security risk, and does not involve patient or confidential information.

7. Unacceptable use

Staff must not use practice email, internet services, devices or systems to:

- create, send, receive, store or access offensive, harassing, obscene, threatening, discriminatory, defamatory or unlawful material;
- access pornography, criminal material, gambling, gaming, private business ventures or other inappropriate websites;
- send confidential or patient information through unauthorised channels;
- send patient information to an unverified recipient or generic / shared inbox without appropriate authority and risk assessment;
- forward practice email to a personal email account;
- use personal email accounts for practice business or patient information;
- share passwords, login credentials, MFA codes or access tokens;
- disable security settings, install unauthorised software or connect unauthorised devices to practice systems;
- store patient information on personal cloud storage, USB drives or personal devices unless specifically approved and secured;
- send bulk unsolicited emails, chain emails, advertisements or political / religious content unrelated to practice business;
- breach copyright, privacy, confidentiality, discrimination or other legal obligations.

8. Patient health information and email

Email may be used for healthcare information only where the communication is appropriate, authorised, documented and managed safely. Secure electronic messaging or approved clinical software functions are preferred for clinical information wherever available.

The practice will not use email for urgent clinical matters. Patients are to be advised that email may not be monitored continuously and is not suitable for emergencies. For urgent symptoms or emergencies, patients must call 000 or seek urgent medical care.

Patient health information must not be sent by standard email unless all of the following are satisfied:

- the request or purpose is legitimate and consistent with the patient's care or practice administration;
- the patient or authorised recipient has been identified and authority to receive the information has been confirmed;
- the recipient email address has been verified before sending;
- the risks of email communication have been explained to the patient where relevant;
- patient consent is recorded in the clinical record where information is being emailed to the patient or another recipient at the patient's request;
- the information is limited to what is necessary;
- attachments are checked before sending;
- password protection, encryption, secure website / portal or secure messaging is used for sensitive information where practicable;
- the communication is saved or documented in the patient record.

9. Patient consent for email communication

Where patient health information is to be emailed to a patient or to a third party at the patient's request, staff must ensure the patient is informed of the risks and that consent is recorded.

Consent should include:

- the email address confirmed by the patient;
- the type of information the patient agrees may be sent by email;
- whether the consent applies once only or on an ongoing basis;
- whether attachments may be sent;
- whether password protection or secure portal access is required;
- that the patient may withdraw consent at any time.

Consent must be documented in the clinical record or approved consent form. Reception or administrative staff must not rely solely on an old email address in the patient file for sending health information.

10. Recipient verification and attachment checks

Before sending any patient-related or confidential information by email, the sender must complete the following checks:

Step	Required check
1	Confirm the patient identity and authority to release information.
2	Confirm the recipient name, role / relationship and reason for receiving the information.

Step	Required check
3	Confirm the email address directly with the patient / recipient or from a trusted source.
4	Do not rely on auto-fill or previous email chains without checking the full address.
5	Check every attachment opens correctly and belongs to the intended patient.
6	Remove unnecessary information and include only what is required.
7	Use password protection / encryption / secure portal or secure messaging when appropriate.
8	Send passwords or access codes by a separate channel, such as phone or SMS, not in the same email.
9	For group emails, use BCC unless all recipients have consented to their addresses being visible.
10	File or document the email in the clinical record where it relates to patient care.

11. Incoming email and online requests

Practice email inboxes and online requests must be monitored during business hours according to practice procedure. They are not emergency communication channels.

The practice maintains an automated email response for the main practice inbox. The response advises senders that the inbox is monitored by non-clinical staff, is not for emergencies or urgent medical matters, provides an expected response timeframe, and directs urgent matters to 000, the nearest emergency department, or telephone contact with the practice.

Staff managing incoming emails must:

- triage messages for clinical urgency and escalate concerns to a GP or nurse promptly;
- confirm patient identity before acting on requests involving patient information;
- document clinically relevant emails in the patient record;
- not provide clinical advice beyond their role or authority;
- avoid confirming sensitive information by email unless the recipient is verified and authorised;
- use approved templates where available for appointment, billing, consent and administrative replies.

> **Suggested auto-reply wording**
>
> Thank you for contacting Donnybrook Family Doctors. This inbox is monitored during business hours and is not for emergencies. If your matter is urgent, call 000 or attend the nearest emergency department. Please do not send sensitive health information by email unless requested by the

practice. We will respond as soon as practicable during business hours.

12. Passwords, MFA and account security

Users must protect practice accounts and systems by following the practice Computer System, Password and Access Policy. Minimum requirements are:

- use unique individual logins; shared accounts are not permitted unless expressly approved for a defined function;
- use strong passwords or passphrases in accordance with practice requirements;
- do not share passwords, MFA prompts, one-time codes or recovery codes;
- enable multi-factor authentication where available and required by the practice;
- lock screens when leaving a workstation;
- log out of systems at the end of use;
- report suspected compromised accounts immediately to the Practice Manager and IT support.

13. Phishing, malware and suspicious emails

All staff must treat unexpected emails, attachments, links, payment requests, password reset prompts and messages requesting patient information with caution.

If an email is suspicious, staff must:

- not click links, open attachments or reply;
- not enter usernames, passwords, MFA codes or patient information into linked websites;
- verify the request by calling a known phone number or using an existing trusted contact method;
- report the email to the Practice Manager and IT support immediately;
- follow IT instructions about deleting, quarantining or preserving the email.

Where a suspicious link or attachment has been opened, the user must immediately disconnect from the network if instructed, stop using the device and notify the Practice Manager and IT support.

14. Devices, mobile access, remote access and BYOD

Practice email or patient information may only be accessed on approved devices and through approved systems. Remote access must be authorised and configured securely.

The following rules apply:

- personal devices must not be used for patient information unless specifically approved and secured;
- mobile phones used for practice email must have screen lock, encryption where available, remote wipe capability where practicable, and must not be shared with family or others;
- lost or stolen devices must be reported immediately;
- public Wi-Fi must not be used for patient information unless a secure VPN or approved secure connection is in place;

- patient information must not be downloaded or stored locally unless necessary, approved and secured;
- remote access must use unique user credentials and MFA where available;
- access must be removed promptly when staff leave or no longer require access.

15. Website, online forms and public information

Only authorised staff may create, edit or approve content on the practice website, online booking pages, social media pages or public-facing online platforms.

Public online information must be accurate, current, professional and consistent with the practice's communication, advertising, privacy and social media policies. Information that may affect patient care, fees, opening hours, services or eligibility must be reviewed before publication and periodically thereafter.

Online forms collecting patient information must be approved by management and must have appropriate security, privacy notices and access controls.

16. Social media cross-reference

Social media use is governed by the practice Social Media and Public Comment Policy. Staff must not post patient information, clinical images, identifiable information from the practice, screenshots, workplace incidents, confidential information or comments that may damage the practice's reputation.

Only authorised staff may respond to online reviews or social media comments on behalf of the practice. Responses must not confirm whether a person is or was a patient.

17. Records and documentation

Email and electronic communications that relate to patient care, clinical decisions, requests, consent, results, referrals, recalls, complaints or significant administrative matters must be saved to, or documented in, the relevant patient record or practice record.

Staff must document:

- patient consent to email health information;
- verification of recipient details where relevant;
- advice given or instructions received by email;
- emails received from third parties requesting patient information;
- disclosure of information and the authority for disclosure;
- incidents, near misses and corrective actions.

18. Privacy, confidentiality and disclosure

Patient and staff information must only be collected, used, disclosed, stored and destroyed in accordance with the Privacy Act, Australian Privacy Principles, relevant health records legislation, professional obligations and practice policy.

Staff must not disclose patient information by email, phone, internet portal or any other electronic method unless the disclosure is authorised, clinically necessary, legally permitted or required, and properly documented.

Requests from insurers, solicitors, employers, police, government agencies, family members or other third parties must be handled under the practice Privacy Policy and Health Information Management Policy. When unsure, staff must escalate to the Practice Manager or Practice Principal before releasing information.

19. Monitoring, audit and compliance

The practice may monitor use of practice systems, email, internet access and devices to maintain security, investigate incidents, meet legal obligations, manage employment obligations and protect patient information.

Breaches of this policy may result in retraining, removal of access, disciplinary action, termination of employment or contract, notification to insurers or regulators, or legal action, depending on the seriousness of the breach.

20. Data breach and cyber incident response

Any suspected privacy breach, email sent to the wrong recipient, lost device, compromised account, malware infection, phishing incident, unauthorised access or accidental disclosure must be reported immediately to the Practice Manager and IT support.

The Practice Manager, Practice Principal and IT support will assess the incident under the practice Data Breach and Cyber Incident Response Procedure, including whether affected individuals, the OAIC, insurers, medical defence organisations or other bodies need to be notified.

Staff must not attempt to conceal or independently resolve a privacy or cyber incident without reporting it.

21. Training and staff acknowledgement

All staff must receive training on this policy at induction and periodically thereafter. Training may include privacy, email risk, phishing, password security, recipient verification, clinical documentation and incident reporting.

Staff must sign the acknowledgement at Appendix C and return it to the Practice Manager for storage in the personnel file or training record.

22. Review

This policy will be reviewed at least annually, or earlier if there are changes to legislation, RACGP Standards, practice systems, email processes, privacy requirements, cyber risks, or following a significant incident or audit finding.

Donnybrook Family Doctors

Appendix A — Before sending patient health information by email

Complete this checklist before sending patient health information by email or attaching patient documents to an email.

Done	Check
☐	Patient identity confirmed.
☐	Authority to release / send information confirmed.
☐	Recipient name and email address verified.
☐	Risks of email explained to patient where relevant.
☐	Consent recorded in the clinical record or consent form.
☐	Information limited to what is necessary.
☐	Correct patient document / attachment selected.
☐	Password protection, encryption, secure portal or secure messaging used where appropriate.
☐	Password / access code sent separately, not in same email.
☐	Email filed or documented in the patient record.

Appendix B — Suggested patient consent note for the clinical record

Suggested clinical note

Patient requested that [describe information / document] be sent by email to [email address / recipient]. Patient identity confirmed. Email address verified with patient. Risks of email communication, including possible unauthorised access or wrong-recipient transmission, were explained. Patient provided consent for this communication. [Password protection / secure method used if applicable.]

Suggested patient-facing wording

Email is convenient but may not be fully secure. There is a risk that information could be sent to the wrong address, intercepted, forwarded, accessed on a lost device, or read by someone other than

the intended recipient. Donnybrook Family Doctors may use secure messaging, password protection or other safer options where appropriate. You can withdraw your consent for email communication at any time.

Appendix C — Staff acknowledgement

I acknowledge that I have read and understood the Donnybrook Family Doctors Email, Internet and Electronic Communication Policy. I agree to comply with the policy, protect patient confidentiality, use practice systems appropriately, report suspected privacy or cyber incidents promptly, and seek guidance if I am unsure about sending or handling information electronically.

Employee / contractor name	_____
Role	_____
Signature	_____
Date	____ / ____ / _____
Manager / witness	_____

Appendix D — Quick reference

Action	Rule
Do	Use secure messaging where available for clinical information.
Do	Verify the recipient email address and attachments before sending.
Do	Record patient consent and relevant communication in the clinical record.
Do	Report suspicious emails and privacy incidents immediately.
Don't	Use personal email for patient or practice information.
Don't	Rely on auto-fill when sending patient information.
Don't	Send passwords in the same email as protected documents.
Don't	Open suspicious links or attachments.
Don't	Confirm patient status or disclose clinical information in online reviews or social media.

Appendix E — Version control and source documents

Version	Date	Summary of change	Approved by
2.0	03 Jun 2026	Updated policy title, scope, patient email communication, consent, recipient verification, attachments, phishing, remote access, privacy, incident response and staff acknowledgement.	Practice Manager
1.0	30 May 2023	Original Email & Internet Policy.	Kaylene Weatherhead

Key source documents used to update this policy:

- RACGP Standards for general practices, 5th edition: Criterion C6.4 — Information security.
- RACGP, Using email in general practice (page last updated 24 March 2026).
- RACGP, Electronic sharing of information (last revised 21 April 2023).
- Office of the Australian Information Commissioner, Australian Privacy Principle 11 — Security of personal information (updated 03 October 2025).
- Practice Privacy Policy, Communication Policy, Health Information Management Policy, Social Media Policy, Data Breach / Cyber Incident Procedure and Computer System / Password Policy.

End of policy