Email and Internet Policy

Version History

Date	Version	Changes	Made By
April 27, 2026	V1.0	Original document	P O'Brien
May 08, 2026	V1.0	No Changes	Board of Management

Introduction

This Email and Internet Policy provides clear guidance on the appropriate, secure, and culturally respectful use of email and internet within Kirrae Health Service (KHS). We are committed to protecting the privacy, dignity, and trust of our clients while ensuring effective communication that supports high-quality, culturally safe healthcare delivery.

KHS recognises the staff requires access to email and the internet to assist in the efficient and safe delivery of healthcare services to our clients. KHS supports the right of staff to have access to reasonable personal use of the internet and email communications in the workplace using the devices and networks provided by the organisation.

Email is an essential communication tool, however, when used incorrectly it can pose risks to confidentiality, information security, and clinical safety.

Purpose

The purpose of this policy is to:

- Ensure email is used safely, professionally, and ethically
- Protect the confidentiality and security of health information
- Support culturally safe communication practices

Policy Objectives

The objectives of this policy are to:

- Safeguard client health information transmitted via email
- Provide clear guidance on acceptable and unacceptable email and internet use
- Reduce the risk of data breaches, miscommunication, and clinical error
- Promote consistency and accountability in organisational communication

Principles

This policy is guided by the following principles:

- Confidentiality: Respect for client privacy and sensitive cultural information
- Cultural Safety: Communication that is respectful, inclusive, and appropriate for Aboriginal and Torres Strait Islander communities
- Security: Protection of information against unauthorised access or disclosure
- Professionalism: Clear, respectful, and appropriate communication at all times
- Accountability: Staff are responsible for appropriate email and internet use

Policy Statement

KHS requires that email and internet be used in a manner that protects client confidentiality, supports clinical safety, and aligns with cultural and ethical responsibilities. Health information must only be shared via email when it is appropriate, secure, and authorised. Personal or insecure email accounts must not be used for clinical or organisational business. Use of the internet by staff and contractors is permitted and encouraged where this supports the goals and objectives of KHS.

Scope
This policy applies to all employees, contractors, students, agency staff, and volunteers, all email systems provided or approved by KHS and all work-related email communications, including internal and external messages. All staff, volunteers and contractors are required to confirm they have understood and agree to abide by this policy.

Definitions

Email
Electronic messages sent and received via systems approved by KHS

Health Information
Information relating to the health, identity, or care of a client, including personal, clinical, and cultural information.

Secure Email
Email systems or methods that use encryption or approved secure messaging platforms to protect sensitive information.

User
Any person authorised to access organisational email systems.

Policy Guidelines and Procedures

Acceptable Use
Users must:

- Use organisational email accounts for all work-related communication
- Ensure emails are clear, respectful, and culturally appropriate
- Include a professional email signature with name, role, organisation and if possible, preferred pronouns
- Verify recipient details before sending emails
- Limited personal use

Limited personal use is permitted where it:

- Is infrequent and brief use
- does not interfere with the duties of other staff or contractors
- does not interfere with the operation of KHS
- does not compromise the security of KHS
- does not impact on KHS's electronic storage capacity or have a high negative impact on our data usage
- does not incur any additional expense for KHS

Any use of internet or email must not violate any legislation or compromise any confidentiality requirements.

Confidentiality and Privacy

- Client-identifiable information must only be sent via secure email systems
- Emails containing health information must be limited to the minimum necessary information
- Consent must be obtained where required before communicating with clients via email
- Email is not to be used for urgent or emergency clinical communication

Clinical Communication

- Email must not replace face-to-face or telephone communication where clinically appropriate
- Clinical advice must be clearly documented in the client's health record if communicated by email
- Automatic disclaimers should state that email is not continuously monitored if this is the case

Information Security

Users must:

- Protect passwords and not share login details
- Log out of email systems when not in use
- Avoid accessing email on unsecured public networks
- Immediately report suspected data breaches or misdirected emails

Prohibited Use

Email or internet must not be used to:

- Send offensive, harassing, obscene, threatening, discriminatory, or culturally inappropriate content
- Transmit confidential information via personal email accounts
- Access or distribute unauthorised or malicious content
- Engage in activities that could damage KHS's reputation
- Visit web sites containing objectionable (including pornographic) or criminal material
- Create, store or exchange information in violation of copyright laws
- Use internet-enabled activities such as gambling, gaming, conducting a business or conducting illegal activities
- Create or exchange advertisements, solicitations, chain letters and other unsolicited or bulk emails
- play electronic or online games in work time

Record Management

- Emails containing clinical or business records must be saved to approved record management systems
- Emails must be retained and disposed of in accordance with organisational record-keeping policies

Breaches and Non-Compliance

Failure to comply with this policy may result in:

- Disciplinary action in accordance with KHS procedures
- Reporting obligations under privacy or health legislation
- Mandatory retraining or system access restrictions

Roles and Responsibilities

Board of Management

- Ensure governance oversight of information security and privacy
- Support policies that protect community trust and cultural safety

Practice Manager and Management Team

- Ensure implementation and regular review of this policy
- Allocate resources for secure email systems and staff training
- Promote compliance with this policy

- Ensure staff understand their responsibilities
- Address breaches promptly

All Staff, Contractors and Volunteers

- Comply with this policy and related procedures
- Maintain confidentiality and cultural respect
- Report breaches or suspected security incidents immediately

KHS I.T Provider

- Maintain secure email infrastructure
- Monitor risks and support incident response
- Provide guidance on secure communication methods

Review

This policy to be reviewed every two years

Related Documents

- KHS Code of Conduct
- KHS Code of Ethics
- KHS Clinical Governance Framework
- KHS Privacy Policy
- KHS Communications Policy
- KHS IT Security Policy
- KHS Risk Management Policy
- Aged Care Statement of rights