Email Policy

Prepared by	IT Services Division
Responsible Officer	Director IT Services
Approving Authority:	FNU Council
Date Approved:	1 August 2025
Next Review:	1 August 2028
Version Number:	1.0

1.0 Introduction

The Fiji National University (FNU) is committed to providing secure Information and Communication Technology (ICT) services to support, enable and enhance its activities.

The Email Policy governs the provision and use of email accounts and the management of the email service platform for both the staff and students of the FNU.

2.0 Abbreviation and Definitions

FNU – Fiji National University

VC - Vice Chancellor

Division – Division of Information Technology Services

DHR - Director of Human Resources

Spam - is defined as unsolicited and undesired advertisements for products or services sent to many users.

Phishing - is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

3.0 Purpose

This policy aims to provide a secure, cost effective and efficient email service including responsibilities of the staff and students of the FNU. This policy is not intended to supersede or replace other University policies but should be read in conjunction with them, especially the Acceptable Use of FNU ICT Resources Policy and ITS User Account and Password Policy.

4.0 Scope

The policy scope applies to all users of email services facilitated by the FNU, including, but not limited to, students, staff, temporary staff, casuals, consultants, contractors, and other parties as approved by the VC.

5.0 Ownership of Email

The University reserves the right to access and monitor email communications when deemed necessary, under the direction of the Director of Human Resources or the Vice Chancellor, in accordance with applicable policies and procedures.

Users will not be provided a copy of the emails upon exiting the University as they remain the intellectual property of the University.

Users are prohibited to setup email forwarding to external non FNU email accounts.

6.0 Statement of Responsibilities

Every user of the email system is responsible for ensuring appropriate and proper usage and must be aware of their responsibilities in this regard. The Division is responsible for the provision, security, and ongoing maintenance of the email system

7.0 Policy Principles

7.1 Provision of Email and Changes

7.1.1 Each staff member and student will be provided with an email address for official work- and study-related communication, respectively. The VC may authorise email access to other parties as deemed appropriate. FNU Staff Email Accounts are created based on the official name of the staff as provided by the HR department. Student accounts are created based on student IDs as per the records with the office of the registrar.

7.1.2 Staff may have multiple email accounts for efficient email access and continuity, known as Official email accounts, which will be based on positions. Staff appointed to acting positions shall be granted access to the relevant substantive email account. The user is required to update the email signature to accurately reflect their acting role. Access to these accounts will be aligned with the expiry date of the staff member's primary account.

7.1.3 The Division shall be responsible for selecting, implementing, and managing the official email platform for all staff and students at the University. This decision will be based on institutional requirements, security considerations, and operational efficiency.

7.1.4 Shared departmental and Special email accounts will be created upon approval from the respective Dean, Director, PVC or VC, as applicable.

7.1.5 Requests for name changes to correct a discrepancy between an email account name and official University records will be processed according to confirmation from the Human Resources division, in which case the email account name will be corrected. This could be due to error or a person legally changing their name.

7.2 Email Storage Size & Deletion

7.2.1 Email data shall be stored on the University's designated online platform. The Division will determine and allocate appropriate mailbox storage limits based on available resources, operational needs, and system capacity. Users are encouraged to delete broadcast emails to free up storage regularly. These measures ensure efficient communication and operation of the email services for all users.

7.2.2 Email messages sent from FNU will have an appropriate sending size limit. This is to ensure emails are sent and received without delay.

7.2.3 After 90 days, the email accounts of students who have completed their program or graduated will be deleted with appropriate awareness.

7.2.4 Staff email accounts will be deleted as per the ITS User Account and Password Policy

8.0 Email Security

The Division employs Email security solutions to protect incoming and outgoing emails. Due to the complex nature of email, it is impossible to guarantee 100% protection against all SPAM and virus-infected messages. It is, therefore, incumbent on everyone to use proper care and consideration to prevent the spread of viruses and avoid falling victim of phishing emails. Users are required to create strong, secure passwords for their email accounts and must not disclose their passwords to any individual, including colleagues. Safeguarding account credentials is the responsibility of each user to ensure the security and integrity of the University's email system.

9.0 Acceptable Use and Best Practice

All email users should be professional in their communications, respond in a timely manner and always adopt best email etiquette practices.

Staff must use the current email signature blocks in accordance with the Signature template designed by the Marketing & Communications team for all email correspondence.

Users must exercise caution when handling unsolicited emails, particularly those from unknown senders. Attachments or links in such emails must not be opened, as they may pose security risks. Additionally, users are prohibited from subscribing to non-work-related mailing lists, forums, or groups using their university email accounts.

All users must promptly report any suspicious or potentially malicious emails to the IT Service Desk for investigation and appropriate action.

10.0 Out-of-office replies

10.1 Staff going on leave.

It is the user's responsibility to set up out-of-office autoreplies prior to going on leave.

10.2 Staff resigning

I It is the responsibility of all departing staff to configure an out-of-office autoreply on their university email account prior to exiting Fiji National University. The autoreply must clearly inform senders of the staff member's departure and provide alternative contact details as advised by their supervisor. Supervisors are accountable for ensuring that this process is completed in a timely and appropriate manner.

10.3 Staff contract terminated.

It is the supervisor's responsibility to ensure appropriate out-of-office auto replies are set up for staff who get terminated. Supervisors may contact IT Service Desk Team for assistance.

11.0 Restrictions and Unacceptable Use and Practice

All users of the University's email system are strictly prohibited from creating, transmitting, or distributing messages that are offensive, disruptive, or inappropriate in nature. This includes, but is not limited to, content containing offensive language or comments relating to race, gender, age, sexual orientation, pornographic material, religious or political beliefs, national origin, or disability.

The dissemination of copyrighted materials without proper authorization, the disclosure of confidential or proprietary information related to Fiji National University operations to unauthorized third parties, or the transmission of any content that may bring the University into disrepute is strictly prohibited.

Users must not use the University's email system to send unsolicited commercial or promotional materials, chain letters, junk mail, or any form of spam. Additionally, the use of university email for political activities—including endorsing or nominating individuals for political parties or public office or attempting to influence the outcome of any election or referendum—is not permitted.

Any user who receives such content or becomes aware of such misuse must immediately report the incident to their Supervisor, Lecturer, or the IT Service Desk for further action.