NIPISSING UNIVERSITY

Policy Category:	General
Policy Number:	1.16.2023.U
Policy Name:	Internal Email Policy
Responsible Department:	Vice-President, Finance & Administration
Approval Date:	September 2023
Approval Authority:	Vice-President, Finance & Administration
Last Updated:	
Review Date:	September 2024

Purpose

The purpose of this email policy is to outline the eligibility, use, and management of the official university email system. All users are expected to familiarize themselves with this policy. Email accounts provided by Nipissing University are intended exclusively for Nipissing University employment-related purposes. This policy does not apply to the student email system or its use.

1.0 Scope

1.1 This policy applies to all users who are provided an official university email account using the domain @nipissingu.ca, including individual, shared, and group email accounts.

2.0 Definitions

2.1 Email: all University IT hardware, software, and services required to accomplish the processing, storage, transmission, and communication of email, whether individually controlled or shared, stand-alone, or networked.

2.2 Official university email account: email accounts using the domain @nipissingu.ca, including individual, shared, and group email accounts.

2.3 Users: all individuals who have an @nipissingu.ca email account.

2.4 UTS: University Technology Services.

2.5 Executive Team: President, Vice-Chancellor; Provost and Vice-President, Academic; Vice-President Finance & Administration

2.6 Departmental authority: person(s) who have signing authority within a unit under the Approval Authority Policy, 2.2.2012.B.

3.0 Policy

3.1 Email Account Eligibility (exceptions may apply)

a. Permanent full-time and part-time employees.
b. Contract employees.
c. Departmental authorities requesting shared or group email accounts.
d. Other accounts as approved by Human Resources, UTS, the Assistant Vice-President, Finance & Infrastructure, or the Vice-President, Finance & Administration.

3.2 Email Account Creation and Designation

a. Requests for email accounts originate from Human Resources and are processed by UTS. Some exceptions may apply.
b. Email accounts are created based on the individual's official name on file with Human Resources.
c. Requests for changes to standard naming conventions are evaluated case-by-case and must be approved by the appropriate departmental authority and UTS.
d. Employees who change job positions at the University may receive a new email account depending on the nature, confidentiality, and/or level of responsibility of their position.
e. Academic administrators will be provided with a new email account for the duration of their appointment. If/when the employee reverts to their faculty position, they will either receive a new email account or revert to their original email.

3.3 Email Account Use

a. All users must follow Nipissing University's Acceptable Use Policy.
b. All users are required to complete all mandatory cybersecurity training to retain access to their official university email account.
c. Email accounts provided by Nipissing University are intended exclusively for Nipissing University employment-related purposes.
d. It is the responsibility of the user to read and act upon, where appropriate, official university email communications.
e. It is the responsibility of the user to ensure the appropriateness of emails they send from their official university email account.

f. Email communications must comply with Canada's Anti-Spam Legislation (CASL), Nipissing University's Respectful Workplace & Learning Environments Policy, and other related policies, legislation, etc.
g. The user shall ensure that they use and manage their official university email account in accordance with Nipissing University policies, procedures, academic regulations, Collective Agreements, etc.
h. Users must ensure they follow Nipissing University email security best practices to protect against unauthorized access to their email account, which include;
    - Not sharing their username and/or password with anyone;
    - Not reusing their username and/or password anywhere else;
    - The use of mandatory multifactor authentication (MFA);
    - Not forwarding or transferring their emails to a non-University email account.
i. The University maintains identifiable email groups for ease of communication to specific groups, for which there is no opt-out option. Some groups have limited sender and "Reply All" functionality.
j. The use of departmental email accounts for general departmental operations is strongly encouraged for business continuity purposes.
k. Departmental email accounts and groups are under the management of the departmental authority. The departmental authority is responsible for the approval, membership, and appropriate use of general email accounts within their department, including maintaining current membership.

3.4 Email Account Management

a. UTS is responsible for instituting appropriate email security measures to safeguard University data and systems.
b. UTS is responsible for taking appropriate action when malicious emails threaten the security of University data or systems or otherwise have the potential to cause harm, which includes but is not limited to;
    - Blocklisting the sender;
    - Purging malicious emails from the system;
    - Locking email accounts that may be compromised.
c. UTS is responsible for taking appropriate action in situations where intentional or unintentional use of the email system negatively impacts University operations.
d. If there is reason to suspect that laws or University policies have been or are being violated or that continued access poses a threat to the facility, other users, normal operations, or the reputation of the University, access privileges of any user may be withdrawn or restricted.
e. An employee's reasonable expectation of privacy is subject to the University's right to access email records for distinct purposes, including but not limited to;
    - Activities outlined in Nipissing University's Electronic Monitoring Policy;
    - A request under the Freedom of Information and Protection of Privacy Act;

- To recover evidence while investigating allegations of misconduct;
- To manage actual or potential criminal or civil litigation in which the University is or may become a party and/or
- To mitigate a threat to the University's information/system security.

f. In the event of an extenuating circumstance where a request to access the contents of a user's email is required, approval must be obtained by an Executive team member.
g. Departmental authorities may request access to the email account of a user they supervised who no longer uses that email account or no longer works at the University for business continuity purposes.

3.5 Account Retention and Dissolution

a. When non-faculty employees leave the University, whether by resignation, termination, end of contract, or retirement, they do not retain access to their university email account. Upon departure from the university, all account and service access is removed with the exception of limited guest access to WebAdvisor for access to required tax information.
b. The Contract Academic Staff Bargaining Unit (CASBU) and Nipissing University Faculty Association Full-time Academic Staff Bargaining Unit (NUFA or FASBU) collective agreements outline email account retention. Upon departure from the university, all other account and service access is removed with the exception of limited guest access to WebAdvisor for access to required tax information.

4.0 Enforcement

4.1 Failure to comply with this policy may result in employment consequences , including disciplinary action and/or termination.

Any exceptions to this policy can be made at the discretion of the Vice-President, Finance & Administration.

QUESTIONS?

Questions about this policy should be directed to the Vice-President, Finance & Administration at **vpfa@nipissingu.ca**.