# RULES AND GUIDELINES FOR THE USE OF ELECTRONIC MAIL

> ***Please take note of the content of this document together with the***
> [***Guidelines regarding Email Etiquette***](link)***.***

## 1    Governance, management, and implementation

This rules and guidelines are overseen by Information Technology and will be reviewed on a regular basis.

## 2    Purpose and Objectives

The purpose and objectives of the rules and guidelines are to:

2.1    Ensure the proper use of the e-Mail service by the NWU. It applies to any corporate e-Mail system, as a service, that the NWU has or may install currently and in future. Employees and students have the responsibility to use e-Mail in an efficient, effective, ethical, and lawful manner. e-Mail users must follow the same code of conduct expected in any other form of written or face-to-face business and academic communication.  The NWU also allows the use of corporate e-Mail for personal communication.

2.2    Provide standards to all staff and students for the acceptable and appropriate use of the e-Mail system, as a service provided by the NWU

2.3    To ensure data protection through the management of e-Mail platform as information resource.

2.4    To mitigate against liability by setting boundaries for appropriate user conduct when using the e-Mail provided by the NWU.

2.5    To safeguard the e-Mail system from misuse, abuse, damage, or disruption.

2.6    To ensure that users understand that the e-Mail service is provided to them primarily for official NWU business and academic use.

## 3    Employee and Student Responsibilities

### 3.1    Acceptable e-Mail Uses

3.1.1    Communicating in a professional manner with other NWU staff and students about work-related matters.

3.1.2    Communicating in a professional manner with parties outside the NWU for business and academic purposes.

3.1.3    Personal communication that are brief and do not interfere with work responsibilities.

3.1.4    Electronic messages are frequently inadequate in conveying mood and context. Users should carefully consider how the recipient might interpret a message before composing or sending the message.

### 3.2    Unsolicited bulk e-Mails

The following is prohibited:

3.2.1    Bulk unsolicited mail, commercial advertising of other businesses, mail-flooding, or excessive cross postings on newsgroups, internally or externally.

3.2.2    The use of any computer resource to promote any business or enterprise, except that of the University, unless such use is explicitly permitted by an agreement between the employee and the University.

3.2.3    Consume more than a trivial number of resources or affect the availability of the system.

### 3.3 Unacceptable e-Mail Uses

3.3.1 Creating and exchanging messages that can be interpreted as offensive, harassing, obscene, racist, sexist, ageist, pornographic or threatening, as defined by the NWU's code of conduct.

3.3.2 Creating and exchanging information that is in violation of copyright or any other law. The NWU is not responsible for an associate's use of e-Mail that breaks laws or obstruction of justice.

3.3.3 Personal communications that interfere with work responsibilities.

3.3.4 Opening file attachments from unknown or untrustworthy sources, or with suspicious or unexpected subject lines.

3.3.5 Sending confidential information to unauthorized people or violating the NWU's data protection policy. Otherwise using e-Mail in a way that increases the NWU's legal and regulatory liability.

3.3.6 Communications that strain the NWU's network or other systems unduly, such as sending large files to large distribution lists, especially not related to business or academic work.

3.3.7 Communications to distribution lists of only marginal interest to members and replying to the entire distribution list when a personal reply is as effective as necessary.

3.3.8 Communications with non-specific subject lines, with in-articulate language and without clear purpose.

3.3.9 Forwarding work-related e-Mail messages to personal accounts, because of unacceptable risks associated with privacy, security and compliance.

3.3.10 Using any e-Mail system or service, other than the NWU e-Mail system, for institutional related communications.

3.3.11 Circulating chain letters and/or commercial offerings that are not the NWU's official business.

3.3.12 Circulating personal information of staff, students and/or colleagues in violation of POPIA.

3.3.13 Promoting or publishing an employee's or student's political or religious views, operating a business other than the NWU's one, or for any undertaking that offers personal gain.

### 3.4 e-Mail Content

3.4.1 Users are forbidden to use any email template, banner, background etc. that is not approved for use by the NWU.

3.4.2 All users are required to identify themselves with an attached signature approved and standardized by the NWU.

3.4.3 The standard NWU e-Mail Disclaimer will be attached to all messages originating from the NWU's e-Mail System with the Domain Name System (DNS) - domain name: nwu.ac.za. NWU Corporate Communication is responsible for supplying the disclaimer.

3.4.4 Users acknowledges that, in terms of the ECT Act, all e-Mails sent or received, and all electronic transactions are legally binding and enforceable in a court of law.

## 4 Privacy Guidelines

The NWU has an obligation to fulfil responsibilities under the laws and regulations of the jurisdictions in which it operates within — for example, to supply information to regulators and/or to supply information in criminal investigations, when required by the law. The NWU has the responsibility to protect its communication infrastructure and the following amenities must be covered:

4.1 On termination or separation, the NWU will immediately deny access to e-Mail, including the ability to download, forward, print or retrieve any message stored in the system, regardless of sender or recipient.

4.2 Employees who leave the NWU will have their mailboxes deleted after one-calendar month of their exit date. The employee's manager may request that access be given to another employee who may remove any needed information within the same one-month time frame.

4.3 The NWU reserves the right to archive and review all messages in an employee's e-Mail account. If the NWU needs to intercept, monitor, or disclose any messages (for example, to comply with legal requirements/regulations or for technical reasons), then it must obtain individual and explicit consent of the employee. If this is not possible — e.g., where informing the suspect would interfere with criminal

investigations — then the NWU must involve and get permission from Internal Audit, People and Culture, University Management Committee (UMC) or Council – whichever is relevant for a particular case.

4.4     The NWU reserves the right to alter, modify, re-route, or block the delivery of messages as necessary to protect communications. This includes, but is not limited to:

4.4.1   Rejecting, quarantining, or removing attachments and/or malicious code from messages that may pose a threat to NWU resources.

4.4.2   Appending legal disclaimers to messages.

4.5     Any content created with the e-Mail system is considered the intellectual property of the NWU.


# 5     Security

As with any other type of software that runs over a particular network, e-Mail users have the responsibility to follow sound security practices:

5.1     Users should not use e-Mail services to transfer sensitive data, such as usernames, passwords and account numbers over the Internet. They should not use the e-Mail system to transfer sensitive data, except in accordance with the NWU data protection policies. Sensitive data passed via e-Mail over the Internet could be read by parties other than the intended recipients, particularly if it is clear text. Malicious third parties could potentially intercept and manipulate e-Mail traffic.

5.2     In an effort to combat the propagation of e-Mail viruses, certain attachment types may be stripped at the NWU e-Mail gateway. Recipients will be notified via e-Mail when this occurs. Should this create a business or academic hardship, users should contact the help desk.

5.3     Attachments can contain viruses and other malware. Users should only open attachments from known and trusted correspondents. Suspicious attachments should be forwarded to the IT helpdesk.

5.4     Spam is automatically filtered at the NWU gateway in a highly efficient manner. e-Mails that are clearly identified as spam before receiving them at the gateway will be deleted (e.g., based on a domain blacklist). All e-Mails that are received by the company's e-Mail gateway will be delivered to the employees or students. Suspicious e-Mails are put in a local spam folder. The employee is responsible for reviewing this folder regularly, deleting and processing business or academic e-Mails that were filtered wrongly.

5.5     NWU IT or any other company group associated with the NWU will not ask for personal information, such as usernames or passwords, by e-Mail. Any such requests should be forwarded to the IT helpdesk. Such approaches — known as "phishing" — are fraudulent approaches carried out for the purpose of unlawful exploitation.


# 6     Operational Guidelines

The NWU employs certain practices and procedures in order to maintain the health and efficiency of electronic messaging resources, to achieve its business and academic objectives, and/or to meet various obligations and regulations. These practices and procedures are subject to change, as appropriate and/or required under evaluated and approved circumstances.

Employees and students are allocated storage space for e-Mail, dependant on the system used and available resources. Users will be unable to send messages when their mailbox exceeds the allocated limit. Users are expected to perform regular clean-up activities to remain within the allocated limits. The IT Service Desk is available to offer best practices in reducing mailbox size and alternatives for additional storage.


# 7     Managing e-mails as records

All e-mails that fit the definition of a record as contemplated in the NWU Records Management Programme must be regarded as an official record of the NWU and must be managed in keeping with the NWU Records Management Policy, related processes/procedures and the NWU File plan and disposal schedule.

A guideline for managing records as e-mails will be made available to staff members to ensure that all staff members are aware of their responsibilities in this regard. The guideline will be updated on an annual basis and/or sporadically if and when required as amendments are made to the related policies, procedures and legislation.

It is the responsibility of all staff members and student leadership to ensure that e-mails that are regarded as records must be managed, stored and disposed of as contemplated in the NWU Records Management Programme.