IT – Email Policy

1. Introduction 1
2. Scope 1
3. Access 1
4. Acceptable Use 2
5. Personal Use 2
6. Prohibited use 2
7. Privacy, Security and Confidentiality 3
8. Penalties for Improper Use 4

1. Introduction

1.1 Email is an important means of communication for NMITE and needs to be managed and used appropriately. The purpose of this document is to set out NMITE's policy on the use of email to:

i. Establish rules on acceptable use of email

ii. Safeguard the operation of the email facilities and minimise risk of disruption to those facilities

iii. Clarify issues of privacy, ownership, and security of electronic communications.

2. Scope

2.1 The policy applies to all email facilities provided either directly by NMITE or their approved suppliers, including any operated by departments or satellite locations, home use or third-party locations/facilities. It applies to all users of these facilities.

3. Access

3.1 Only staff, students and other persons authorised by appropriate NMITE authority are entitled to use NMITE's email systems and resources. If IT facilities are misused access may be withdrawn in line with the NMITE disciplinary procedures.

4. Acceptable Use

4.1 NMITE email facilities are provided to support the Institute's activities including but not limited to learning, teaching, research, administration, and approved business activities. Email must be used responsibly and in compliance with the law and with all NMITE's regulations and policies. All users are subject to these regulations governing the use of computing facilities.

4.2 Use of email requires the same care and imposes the same obligations as any other medium of communication. As a written medium, it may remain in the sender's and the recipient's file store and on backup media, and in transit it may be observed in much the same way as a postcard.

4.3 Although all inbound emails are scanned using anti-spam and virus filtering techniques, it must not be assumed that all email traffic is therefore trouble free. Techniques are prevalent for disguising and cloaking malicious content and it is the user's responsibility to ensure that all reasonable precautions are undertaken before viewing content, whether in the email body, linked or especially in attachments. Should you have reason to suspect a message, it is also important to ensure that appropriate IT contact is informed and that the email is not forwarded to anyone since they may misconstrue your intent and trust your email is safe.

5. Personal Use

5.1 NMITE permits reasonable personal use of email facilities. Reasonable use means use that does NOT:

i. create an identifiable cost to NMITE

ii. interfere with use of email for NMITE purposes

iii. adversely impact the work of any employee

iv. conflict with NMITE objectives or interests

v. conflict with obligations between NMITE as employer and individual as employee/contractor

vi. involve personal financial gain or non-institutional commercial/profit making activities

5.2 Any such personal use is subject to NMITE regulations and the provisions of this policy and as such, is subject to review and modification.

6. Prohibited use

6.1 NMITE email facilities may NOT be used for:

i. the creation, transmission or storage of text, images or other material which could be considered offensive such as pornographic, unlawfully discriminatory, or libellous material.

ii. harassment of any person or group of persons

iii. production or promulgation of material which could bring NMITE into disrepute.

6.2 Where such a legitimate situation arises, prior permission must be sought in writing from the appropriate authorised senior manager in the case of academic activity and from the Registrar in respect of any other matter.

i. undertaking, assisting, or encouraging a criminal act

ii. the transmission of unsolicited commercial email or bulk non-commercial e-mail unrelated to the legitimate educational activities of NMITE which is likely to cause offence or inconvenience to those receiving it (spamming); this includes but is not limited to advertisements and political and religious materials

iii. emails which purport to come from an individual other than the user, who sends the message, or with forged addresses (spoofing)

iv. unauthorised transmission to a third party of confidential material concerning the activities of NMITE.

v. transmission of material that infringes copyright including intellectual property rights

vi. personal gain or commercial purposes unrelated to the legitimate activities of NMITE

vii. Unreasonable or excessive personal use – see above

viii. distribution of virus or malicious software

7. Privacy, Security and Confidentiality

7.1 Users should be aware that:

i. email is not a secure medium and could be seen by someone other than by the intended recipient, including systems administrators carrying out their normal support duties. It is not advisable to send confidential information via email

ii. NMITE does not routinely monitor email content but may make interceptions and inspections in certain circumstances within the law. These include the investigation of incidents, such as cases where there are reasonable grounds for believing there has been a contravention of rules, regulations or the law, and the investigation of abnormal systems behaviour. For more details of see Investigatory Powers Act, 2016[1]

iii. in the event of unplanned absence and access being required to email held in a user's account reasonable efforts must be made to contact the account holder and seek an agreed means of access to the material. In circumstance where such arrangements cannot be agreed, and with due regard for the importance and urgency of the situation, the authorised senior manager can request privileged access be granted. Such access will be subject to NMITE's Email Mail Policy and limited to the stated need.

iv. email containing personal information comes within the requirements of GDPR and the Data Protection Act which includes the need for disclosure, on request, to the subject of that information

v. email credentials can be forged so messages received might not be from the purported sender

vi. messages may be retrievable from backup, even when the sender and recipient have both deleted their copies. However, this policy does not require holders of backup material to provide a retrieval service.

vii. NMITE retains all rights to information transmitted and held within the email system, including but not limited to intellectual property.

7.2 Users may not, under any circumstances, monitor, intercept or browse other users' e-mail messages unless authorised to do so.

7.3 Network and computer operations personnel, or system administrators, may not monitor or view other users' e-mail messages other than to the extent that this may occur incidentally in the normal course of their work e.g., postmasters may need to inspect messages when dealing with delivery failures. Where they are asked to monitor or view email to investigate an incident (see second bullet point above) this will require the permission of the Registrar, the authorised senior manager, or the Head of IT.

7.4 NMITE reserves the right to access and disclose the contents of a user's e-mail messages, in accordance with its legal and audit obligations, and for legitimate operational purposes. NMITE reserves the right to demand that encryption keys, where used, are made available so that it can fulfil its right of access to a user's e-mail messages in such circumstances.

8. Penalties for Improper Use

8.1 Refer to the NMITE disciplinary policy