IT – Information Security Policy

1. Purpose

1.1 The purpose of this Policy is to safeguard information belonging to NMITE and its stakeholders (third parties, clients or customers and the general public), within a secure environment.

1.2 This Policy informs NMITE’s staff, students, and other individuals entitled to use its facilities of the principles governing the holding, use and disposal of digital information.

1.3 It is the goal of NMITE that:

i. Information will be protected against unauthorised access or misuse.

ii. Confidentiality of information will be secured.

iii. Integrity of information will be maintained.

iv. Availability of information / information systems is maintained for service delivery.

v. Business continuity planning processes will be maintained.

vi. Regulatory, contractual, and legal requirements will be complied with.

vii. Physical, logical, environmental and communications security will be maintained.

viii. Infringement of this Policy may result in disciplinary action or criminal prosecution.

ix. When information is no longer of use, it is disposed of in a suitable manner.

x. All information security incidents will be reported to the Director of IT and investigated through the appropriate management channel(s).

1.4 Information relates to:

i. Electronic information systems (software, computers, and peripherals) owned by NMITE whether deployed or accessed on or off campus.

ii. NMITE’s computer network used either directly or indirectly.

iii. Hardware, software, and data owned by NMITE.

iv. Paper-based materials.

v. Electronic recording devices (video, audio, CCTV systems).

2. The Policy

NMITE requires all users to exercise a duty of care in relation to the operation and use of its information systems.

2.1 Authorised users of information systems

2.1.1 With the exception of information published for public consumption, all users of NMITE information systems must be formally authorised by appointment as a member of staff, by enrolment as a student, or by other process specifically authorised by specified NMITE management. Authorised users will be given a unique user identity. Any password associated with a user identity must not be disclosed to any other person.

2.1.2 Authorised users will pay due care and attention to protect NMITE information in their personal possession. Confidential, personal, or private information must not be copied or transported without consideration of:

i. Permission of the information owner.

ii. The risks associated with loss or falling into the wrong hands.

iii. How the information will be secured during transport and at its destination.

2.2 Acceptable use of information systems

2.2.1 Use of NMITE's information systems by authorised users will be lawful, honest and decent and shall have regard to the rights and sensitivities of other people.

2.3 Information System Owners

2.3.1 Key NMITE staff who are responsible for information systems are required to ensure that:

i. Systems are adequately protected from unauthorised access.

ii. Systems are secured against theft and damage to a level that is cost-effective.

iii. Adequate steps are taken to ensure the availability of the information system, commensurate with its importance (Business Continuity).

iv. Electronic data can be recovered in the event of loss of the primary source. I.e. failure or loss of a computer system. It is incumbent on all system owners to backup data and to be able to restore data to a level commensurate with its importance (Disaster Recovery).

v. Data is maintained with a high degree of accuracy.

vi. Systems are used for their intended purpose and that procedures are in place to rectify discovered or notified misuse.

vii. Any electronic access logs are only retained for a justifiable period to ensure compliance with the data protection, investigatory powers, and freedom of information acts.

viii. Any third parties entrusted with NMITE data understand their responsibilities with respect to maintaining its security.

2.4 Personal Information

2.4.1 Authorised users of information systems are not given rights of privacy in relation to their use of NMITE information systems. Duly authorised staff in NMITE may access or monitor personal data contained in any NMITE information system (mailboxes, web access logs, file-store etc).

2.4.2 Individuals in breach of this policy are subject to disciplinary procedures (staff or student) at the instigation of the NMITE staff with responsibility for the relevant information system, including referral to the Police where appropriate.

2.4.3 NMITE will take legal action to ensure that its information systems are not used by unauthorised persons.

3. Ownership

3.1 The Director of IT has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.

3.2 Information system owners are responsible for the implementation of this Policy within their area, and to ensure adherence.

Author of Policy	Director of IT
Equality Impact Assessment (Equality Analysis) completed	26/06/2020
Date Policy (Re)Approved	
Version Number	5.0
Approval Authority	Executive Board
Date of Commencement	Feb2020
Amendment Dates	July 2023
Reason for update	Annual review
Date for Next Review	July 2025
Related Policies, Procedures, Guidance, Forms or Templates	N/A
Policies/Rules Superseded by this Policy	V1.0: Feb 2020 V2.0: Aug 2020 V3.0: June 2021 V4.0: July 2022
Summary of changes made to this version	Changed Head of IT to IT Director Version controlled