IT – Acceptable Use Policy

Table of Contents

1. Introduction

1.1 This Acceptable Use Policy applies to all NMITE employees, students, contractors and agents (hereafter referred to as 'individuals'). By accessing or using NMITE IT facilities you agree to be bound by this policy.

1.2 This policy stipulates what individuals may and may not do when using NMITE's IT resources, the legal requirements, and the consequences of breaking the rules.

1.3 This policy covers the use of all NMITE IT resources and should be interpreted such that it may include new and developing technologies and uses, which may not be explicitly referred to.

1.4 It is the responsibility of all individuals using NMITE IT services to read and understand this policy.

1.5 This policy will be reviewed at least annually, in line with NMITE Policy Framework, and may be updated in to comply with legal and policy requirements.

1.6 In addition to this policy all individuals using NMITE's IT must adhere to the Janet Acceptable Use Policy and the Janet Security Policy, published by Janet (UK).

2. Scope

2.1 This Policy is intended to define a clear basis for the use of NMITE IT resources, whether provided directly, or through nominated service providers. Although individual IT resources may not all be referred to individually in this document, it should be interpreted to incorporate all digital hardware, systems, and solutions at NMITE.

2.2 This policy document forms part of the NMITE core policies and must be accepted in conjunction with other relevant policy documents.

2.3 Any lists of acceptable/unacceptable usage, equipment, conditions, etc. enclosed within this policy do not form an exhaustive list. Other related incidents will be approached appropriately, on a case-by-case basis.

3. Policy

3.1 User Credentials

3.1.1 Access to NMITE IT systems is controlled using user IDs and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the NMITE IT systems.

Individuals must not:

i. Allow anyone else to use their user NMITE ID and password, or any other NMITE IT system credentials.

ii. Use someone else's user ID and password to access NMITE IT systems.

iii. Leave their user accounts logged in at an unattended and unlocked computer.

iv. Leave their password unprotected (for example writing it down).

v. Perform any unauthorised changes to NMITE IT systems or information.

vi. Attempt to access data that they are not authorised to use or access.

vii. Exceed the limits of their authorisation or specific business need to interrogate the system or data.

viii. Store NMITE data on any non-authorised NMITE equipment.

ix. Give or transfer NMITE data or software to any person or organisation outside NMITE without the authority of NMITE.

x. Those with supervisory responsibilities must ensure that individuals are given clear direction on the extent and limits of their authority about IT systems and data.

3.2 Internet and email

3.2.1 Use of NMITE internet and email is intended for business/learning purposes. Personal use is permitted where such use does not affect the individual's business/learning performance, is not detrimental to NMITE in any way, not in breach of any term and condition of employment/student regulations and code of conduct and does not place the individual or NMITE in breach of statutory or other legal obligations.

3.2.2 All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

i. Use the internet or email for the purposes of harassment or abuse.

ii. Use profanity, obscenities, or derogatory remarks in communications.

iii. Access, download, send or receive any data (including images), which NMITE considers offensive in any way, including sexually explicit, discriminatory, defamatory, or libellous material.

iv. Use the internet or email to make personal gains or conduct a personal business.

v. Use the internet or email to gamble.

vi. Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.

vii. Place any information on the Internet that relates to NMITE, alter any information about it, or express any opinion about NMITE, unless they are specifically authorised to do this.

viii. Send unprotected sensitive or confidential information externally.

ix. Forward NMITE mail to personal (non-NMITE) email accounts (for example a personal GMail account).

x. Make official commitments through the internet or email on behalf of NMITE unless authorised to do so.

xi. Download copyrighted material such as music media (MP3) files, film, and video files (not an exhaustive list) without appropriate approval.

xii. In any way infringe any copyright, database rights, trademarks, or other intellectual property.

xiii. Download any software from the internet without prior approval of the IT Department.

xiv. Connect NMITE devices to the internet using non-standard connections.

xv. carry out any hacking activities; or

xvi. intentionally or recklessly introduce any form of spyware, computer virus or other potentially malicious software.

3.3 Clear Desk and Clear Screen Policy

3.3.1 To reduce the risk of unauthorised access or loss of information, NMITE enforces a clear desk and screen policy as follows:

i. Personal or confidential business information must be protected using security features provided for example secure print on printers.

ii. Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.

iii. Care must be taken to not leave confidential material on printers or photocopiers.

iv. All business-related printed matter must be disposed of using confidential waste bins or shredders.

3.4 Working Off-site

3.4.1 It is accepted that laptops and other mobile devices will be taken off-site. The following controls must be applied:

i. Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.

ii. Laptops must be carried as hand luggage when travelling.

iii. Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.

iv. Care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones, and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

v. *Specific to employees* - working away from the office must be in line with NMITE remote working policy. Mobile storage devices such as memory sticks, CDs, DVDs, and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only NMITE authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

3.5 Software

3.5.1 Individuals must use only software that is authorised by NMITE. Authorised software must be used in accordance with the software supplier's licensing agreements.

3.5.2 All software on NMITE computers must be approved and installed by the NMITE IT department.

3.6 Viruses, phishing, and anti-malware software

3.6.1 The NMITE IT department has implemented centralised, automated virus detection and anti-malware software updates. All NMITE PCs have antivirus software installed to detect and remove any virus and malware automatically.

Individuals must not:

i. Attempt to remove or disable anti-virus software.

3.7 Telephony (Voice) Equipment Conditions of Use

3.7.1 Use of NMITE voice equipment is intended for business use. Individuals must not use NMITE voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications

Individuals must not:

i. Use NMITE voice for conducting private business, unless in exceptional circumstances.

ii. Make hoax or threatening calls to internal or external destinations.

iii. Accept reverse charge calls from domestic or international operators, unless for business use.

4. Actions upon Termination of Employee or Student Contract

4.1 All NMITE equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to NMITE at termination of contract.

4.2 All NMITE data or intellectual property developed or gained during the period of employment remains the property of NMITE and must not be retained beyond termination or reused for any other purpose.

5. Monitoring and Filtering

5.1 All data that is created and stored on NMITE resource is the property of NMITE and there is no official provision for individual data privacy, however wherever possible NMITE will avoid opening personal emails.

i. IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. NMITE has the right (under certain conditions) to monitor activity on its systems, including internet and email use, to ensure systems security and effective operation, and to protect against misuse.

ii. Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000, and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

5.2 By using NMITE facilities, all users are also bound to legislation, including but not limited to.

i. Data Protection Act 2018 (incorporating GDPR 2018) - link

ii. Investigatory Powers Act 2016 - link

iii. Malicious Communications Act 1988 - link

iv. Computer Misuse Act 1990 - link

v. Freedom of Information Act 2000 - link

By using the approved Third-Party facilities offered through NMITE, all users are also bound by further Acceptable Use Policies, including but not limited to,

i. JISC Janet Acceptable Use Policy - link

Individuals have a responsibility to report suspected breaches of security policy without delay to your line management, Personal Tutor, the IT department, the information security department, or the IT Service Desk.

6. Legalities and Prohibited Use

6.1 You must not use NMITE IT facilities in any way that could expose you or NMITE to any criminal or civil liability.

6.2 NMITE has a statutory duty of care, under Section 26 of the Counter Terrorism and Security Act 2015, termed “PREVENT”. The purpose of this duty is to aid the process of preventing people from being drawn into terrorism.

6.2.1 Extremist material - in compliance with Section 26 of the Counter-Terrorism and Security Act 2015, staff, students and visitors using NMITE IT systems must not create, transmit, receive, view or store material with such intent to radicalise themselves or others. If a member of the NMITE community believes they may have encountered a breach of this provision, they should immediately contact the PREVENT lead (Sam Lewis, HR Director) or in their absence the Academic Registrar (Tam Milner) .

6.3 Computer misuse – unauthorised access to accounts, programs and/or data (including copying, corrupting, or deleting) and all forms of hacking are prohibited and may be an offence under the Computer Misuse Act 1990.

7. Consequences of Breach

7.1 Refer to the NMITE disciplinary policy