IT – Acceptable Usage Policy 2020-21

1. Introduction

1.1 This IT Acceptable Usage Policy covers the security and use of all NMITE information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all NMITE employees, students, contractors and agents (hereafter referred to as 'individuals').

1.2 All references to NMITE facilities are to include all IT Resources, Infrastructure, Networking, Telecommunications, Assets, Intellectual Property, Licenses, Services & Systems.

1.3 This policy applies to all information, in whatever form, relating to NMITE business activities worldwide, and to all information handled by NMITE relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by NMITE or on its behalf.

1.4 It is the responsibility of all users of NMITE I.T. services to read and understand this policy. This policy will be reviewed at least annual in line with NMITE Policy Framework and may be updated in addition, in order to comply with legal and policy requirements.

1.5 Student will receive a full IT induction within their first week at NMITE

2. Purpose

2.1 This Policy is intended to define a clear basis for the use of NMITE facilities whether provided directly or through nominated Service Providers. Although

facilities may not all be referred to individually in this document, it should be interpreted to incorporate all technologies within 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. Computer Access Control – Individual's Responsibility

3.1 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.

3.2 **Individuals must not:**

i. Allow anyone else to use their user ID and password on any NMITE IT system.

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

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

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. Connect any non-NMITE authorised device to the NMITE network or IT systems.

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

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

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

4. Internet and email Conditions of Use

4.1 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.

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

4.3 **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 Hotmail 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.

5. Clear Desk and Clear Screen Policy

5.1 In order 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.

6. Working Off-site

6.1 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. Particular 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.

7. Specific to employees - working away from the office must be in line with NMITE remote working policy. Mobile Storage Devices

7.1 Mobile 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.

8. Software

8.1 Individuals must use only software that is authorised by NMITE on NMITE computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on NMITE computers must be approved and installed by the NMITE IT department.

8.2 **Individuals must not:**

i. Store personal files such as music, video, photographs or games on NMITE IT equipment.

9. Viruses, phishing and malicious software

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

9.2 **Individuals must not:**

i. Remove or disable anti-virus software.

ii. Attempt to remove virus-infected files or clean up an infection, other than by the use of approved NMITE anti-virus software and procedures.

10. Telephony (Voice) Equipment Conditions of Use

10.1 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

10.2 **Individuals must not:**

i. Use NMITE voice for conducting private business.

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

iii. Accept reverse charge calls from domestic or International operators, unless it is for business use.

11. Actions upon Termination of Employee or Student Contract

11.1 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.

11.2 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.

12. Monitoring and Filtering

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

12.2 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, in order to ensure systems security and effective operation, and to protect against misuse.

12.3 Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

12.4 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

12.5 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

12.6 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 helpdesk.

13. Consequences of Breach

13.1 All breaches of information security policies will be investigated.

13.2 In the event of a breach of this Acceptable Usage Policy by an individual NMITE may in its sole discretion:

i. restrict or terminate an individuals right to use the NMITE network;

ii. withdraw or remove any material uploaded by that individual in contravention of this Policy; or

iii. where appropriate, disclose information to law enforcement agencies and take any legal action against aa individual for breach of this Policy, including but not limited to claiming all costs, fees and disbursements (including but not limited to legal fees) connected therewith.

13.3 In addition, where investigations reveal misconduct, disciplinary action may follow in line with NMITE disciplinary procedures.

Employee Disciplinary Policy and Procedure

Student Disciplinary Policy

14. Policy Status

13.1 This policy is not part of any contract of employment or student contract and does not create contractual rights or obligations. NMITE reserves the right to alter at any time although we will notify you of any future amendments.

Agreement to adhere to the Acceptable Use Policy:

I confirm that I have received a copy, read and understand that I must adhere with the above policy and understand that any breach could result in disciplinary action.

I will **immediately** report the loss of any equipment covered by this policy to NMITE IT Support

I will report any incidents of concern regarding misuse of technology/software/social media to my line manager/Personal Tutor in the first instance.

I understand that the organisation will monitor the use of IT systems including email and other digital communications.

Name:……..

Signed: ……

Position: ……