IT – Bring Your Own Devices (BYOD) Policy 2020-21

1. Introduction 1
2. Scope 1
3. Responsibilities 2
4. Storage 2
5. Removable devices and media 3
6. Consequences of breaching this policy 3

Agreement to adhere to the BYOD Policy: 4

1. Introduction

1.1 It is recognised that in addition to NMITE provided IT devices, that students and staff may use personal devices to undertake elements of their study and work. This BYOD Policy has been developed to help foster and promote a suitable and secure learning/working environment.

1.2 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.

1.3 Individuals using a BYOD must adhere to all other relevant IT related NMITE policies:

i. Acceptable Usage Policy
ii. Information Security Policy
iii. Electronic Mail Policy
iv. Data Protection Policy
v. Security and Data Backup Policy

2. Scope

2.1 This policy applies to all NMITE employees, students, visitors, contractors and agents (throughout referred to as ‘individuals’).

2.2 This Policy is intended to define a clear basis for the use of all personal devices belonging to individuals which are connecting to NMITE facilities and services via the Wireless Network.

2.3 Such devices include, but are not limited to, smart phones, tablets, laptops, servers, portable hard drives, USB sticks or any other fixed or mobile computing device.

3. Responsibilities

3.1 Before connecting any device to the NMITE wireless network individuals must ensure:

i. that suitable anti-virus and malware protection software.is installed on every device

ii. that suitable encryption software is installed for the storage and access to NMITE provided information

3.2 Individuals using a BYOD must ensure that the operating system and security software is kept up to date at all times.

3.3 Individuals are expected to act responsibly, safely, and respectfully in line with current Acceptable Use Agreements

3.4 Individuals must report the loss of any device containing NMITE data (including email) to IT staff.

3.5 Individuals are advised to arrange appropriate insurance cover for all personal devices.

3.6 NMITE takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding BYODs. NMITE will not be responsible for any loss or damage resulting from any support given or advice provided.

3.7 NMITE reserves the right to refuse, prevent or withdraw access to devices where it considers there to be an unacceptable security, or other risk.

3.8 NMITE reserves the right to access BYODs where it is suspected that there has been a security breach or a breach of any NMITE policy.

3.9 Individuals using a BYOD will need to co-operate with IT staff should it be necessary to access or inspect the device.

4. Storage

4.1. Devices with synchronised online storage present considerable opportunities for data loss or inappropriate use or access to information. Individuals therefore must ensure the following:

4.1.1. Where NMITE has provisioned cloud storage (e.g. OneDrive) individuals are expected to utilize these services in favour of any other storage option.

4.1.2 No sensitive or important information should be synchronised to or stored on cloud based storage that has not been provided by NMITE. This includes but is not limited to:

i. GoogleDocs

ii. Drop box

iii. Skydrive

iv. SugarSync

5. Removable devices and media

5.1. Storage mediums and devices such as USB sticks, external hard drives, flash card and any other portable drives carry considerable risks in transporting, storing, or transferring information and so:

5.1.1. Should not be used unless absolutely necessary to temporarily store information.

5.1.2. Information on such devices should be retained only long enough to fulfil the specific need. As soon as the requirement is completed the information should be fully deleted and unrecoverable from that device.

5.1.3. Encryption should be applied to all such devices.

6. Consequences of breaching this policy

6.1 NMITE will enforce this policy in order to protect those in its care, on its property or using its IT Services.

6.2 Any attempt to violate the provisions of this policy, regardless of the success or failure of the attempt, will, in the case of staff and students, be dealt with under the terms of the relevant disciplinary procedure or policy as applicable to staff and students, and may result in disciplinary action and/or notification to the relevant law enforcement agencies.

6.3 Where a visitor or contractor violates or attempts to violate this policy, their access to NMITE IT systems, wireless network, email and/or internet facilities shall be withdrawn and NMITE will, where appropriate, notify relevant law enforcement agencies. In the case of contractors, NMITE will seek to have the individual removed from services provided to NMITE, on a permanent basis.

6.4 NMITE also reserves the right to withdraw access from all or part of its IT systems, wireless network, email and/or internet facilities where it reasonably believes that this policy is being contravened.

Agreement to adhere to the BYOD 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 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: ……