NUI Galway
OÉ Gaillimh
Policies and Procedures

Code: **QA398**

Title: **Personally Owned Digital Devices (BYOD) Policy**

Review Date: September2020

1. Purpose

The purpose of this policy is to establish standards for the use of **personally owned digital devices** within the National University of Galway.

This policy is intended to protect the security, integrity and availability of National University of Galway's information assets and communications network and to facilitate productivity and convenience to users of the National University of Galway's network.

All users must agree to the terms and conditions outlined in this policy in order to connect their own personal device to the University network.

National University of Galway, here after referred to as NUI Galway reserve the right to revoke access to any user or device if the standards outlined in this document are not adhered to.

2. Scope

This Policy applies to all employees, including permanent and temporary staff, contractors and affiliates who wish to use a personally owned digital devices to access the NUI Galway assets and resources.

Personal devices may include but are not limited to computers, laptops, notebooks, tablets and smart phones.

While NUI Galway recognises the many benefits that the use of personally owned devices brings, it seeks to minimise the risk such devices pose if they are lost, stolen or otherwise compromised; therefore all registered BYOD must be encrypted, password protected and must be capable of having all NUI Galway data remotely wiped in the event of loss or theft.

Registration of a personally owned device for access to the NUI Galway network indicates acceptance of this policy.

3. Definitions

"Must", or the terms **"required"** or **"shall",** refer to an absolute requirement of the policy.

"Must not" or **"shall not",** refer to statements which are an absolute prohibition of the policy.

"Should" or **"recommended"** refer to a statement that should be applied. In certain circumstances, there may be a valid reason to ignore a particular item. In this case the full implications must be understood and carefully weighed before choosing a different course.

“Should not” or **"not recommended"** mean the specified behaviour should not be performed. There may exist valid reasons in particular circumstances when the particular behaviour is acceptable, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

4. Requirements

4.1 Device Registration

Personal digital devices must authenticate against an active campus account before they can access University systems and resources.

In line with the End User Policy, devices (Personal / Non-personal) that are connected to the University network are prohibited from, but not limited to, the following:

- Bypassing security controls deployed by the University (VPN/Proxy servers)
- Impersonation/Fraud
- Phishing
- Insult, Slander and/or defamation
- Network Reconnaissance (Port Scanning, Packet Sniffing etc)
- Torrenting
- Warez sites (Sites that cracks or illegal copies of licenced software)
- Access to the Dark Web
- Hosting personal servers
- Use of relay or networking equipment to retransmit or in any way alter the service provided by the University.

Users may opt out of using their personal device at any time.

NUI Galway takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding personally owned devices.

NUI Galway is not liable for all or any costs that is associated with the use of a personal device.

NUI Galway reserve the right to monitor the use of a personally owned device while it is connected to the university network (e.g. to. monitor data traffic).

4.2 Device Security

To ensure there is no unauthorised access to the NUI Galway network, devices must be encrypted to university standard, capable of being wiped remotely and password protected using the built-in security features of the device as well as a strong password. Please refer to the NUI Galway Password Policy for information on setting a strong password. Please refer to the NUI Galway Encryption Policy for information on encrypting devices.

Extra security measures should be/ are applied as follows:

- Automatically lock after 5 minutes of inactivity
- Hard lock after 5 failed login attempts
- Rooted or Jailbroken devices are forbidden from accessing the network

- Access to NUI Galway data is limited based on user profiles defined by IT and are automatically enforced.
- A device / application may be remotely wiped by NUI Galway if:
    - The device is reported as lost / stolen
    - Employment or association with the University is terminated or expired
    - A policy or data breach, virus or similar threat is detected

4.3 Protection of device and University data

1. Users are encouraged to take regular backups of their devices. In the event of a device being wiped remotely NUI Galway will take **no responsibility for personal data loss.**
2. Users are must keep their software up to date, this includes operating systems, applications, and antivirus malware protection.
3. Users must not connect to the wired network from personal devices.
4. Users must not store confidential NUI Galway information on their personal mobile devices.
5. Users should disable any automated cloud based or local backup services on any devices used to access NUI Galway data.
6. Users must not sync NUI Galway data to their personally owned devices.
7. Users have sole responsibility for ensuring that no other person has access to NUI Galway software or data stored on or being accessed from a personal device.
8. Users recognise that any NUI Galway data stored on their personal device remains the sole property of the NUI Galway.
9. NUI Galway reserve the right to limit or withdraw access to the network and/or it's services at any time without notice.
10. If lost /stolen, all devices with access to the NUI Galway network must be reported to the University IT Department as soon as possible and within 24 hours. (or in line with Data policies)
11. Users must report any suspected data breaches in accordance with the incident reporting procedure:
    https://www.nuigalway.ie/media/oifiganrunai/QA443-Personal-Data-Breach-Procedure-.pdf
12. Any use of a personal device for or in connection with NUI Galway work must be carried out in accordance with NUI Galway's procedures and with any relevant laws.
13. On leaving the university users must ensure that all NUI Galway data is deleted securely from their device.
14. NUI Galway reserve the right to take appropriate disciplinary action up to and including termination for non-compliance with this policy.
15. NUI Galway has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.
16. Cloud storage providers include but are not limited to; OneDrive, Dropbox, Google Drive and iCloud, users should be aware that data stored within these services is being held by a third party. However, responsibility for data security remains with the user and not the cloud storage provider.

5. Reimbursement

NUI Galway does not have a reimbursement policy for personal devices. NUI Galway is not liable for all or any costs associated with the use of a personal device.

6. Supporting Policies / Procedures

QA404 Password Policy

QA406 Remote Access Policy

QA408 Logical Access Policy

QA409 Encryption Policy

QA411 End User Policy

QA443 Personal Data Breech Procedure

7. Policy Review and Approval

Policy Name:	Personally Owned Digital Devices (BYOD) Policy
Policy Owner:	ICT Security Committee Chair
Policy Approved By:	University Management Team
Policy Version:	V1.0
Last Review Date:	September 2020