NUI Galway
OÉ Gaillimh

Policies and Procedures

Code:	QA438 Student Access to IT Services
Title:	Student Access to IT Services
Date:	03/07/2019
Review Date:	03/07/2022
Approval:	ICT Security Committee

1. Purpose

To ensure continuity of our University and to minimise potential for incidents, it is essential that a minimum set of security standards exists to protect the University. This policy is designed to aid in the protection NUI Galway from risks & threats, whether internal or external, deliberate or accidental.

In support of its mission of teaching and research, NUI Galway provides access to computing resources for students and staff of the University. Access to the University's computing facilities is a privilege granted to members of the University which can be withdrawn and which naturally expires when the student or staff member is no longer associated with the University. The University reserves the right to limit, restrict or extend computing privileges and access to its information resources.

The policy is designed to ensure resources are utilised in an effective, efficient, ethical and lawful manner by students of NUI Galway.

This policy relates to the provision of IT Accounts for University students only.

2. Description

This policy applies to:

- All registered NUI Galway Students.

It is the responsibility of students to read this and related security policies and be familiar with their contents. It is the responsibility of staff engaged in teaching learning and research to ensure all students using IT systems are aware of and understand their responsibilities in relation to this policy (and related policies).

3. Definitions

This document provides information security rules and responsibilities for all users of NUI Galway IT systems and as end-user of these systems.

"**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.

"End-User" or **"Member of Staff"** or **"Staff Member"** refers to any employee whether temporary or permanent, NUI employed or Agency employed or an External account holder within any area in NUI Galway.

"Registered Student" refers to a student who is registered on a programme of study, which is delivered completely or in part by NUI Galway.

"ISS" Information Solutions and Services, the Universities designated IT service provider.

4. Requirements

1. Student Accounts

- In general, access to all major IT services for students is supported through a single unique account/identity and password. Information Solutions and Services (ISS) manage this account.
- Students are responsible for all activities carried out using their identity.
- Access to some software is restricted to groups of students and/or specific locations.
- Access to specialist IT services within Schools/Disciplines is administered by the individual unit.
- In the event of a student's account being compromised, the student should take immediate action to resolve the matter including alerting ISS.
- ISS reserves the right to disable/freeze individual accounts where access has been compromised and/or the account poses a threat to the operation of University IT services.

- ISS reserves the right to access individual accounts where it is necessary. This includes but is not limited to the following circumstances:
  - In response to a Freedom of Information or Data Protection request, the University has received and subject to the approval of the Freedom of Information or Data Protection Officer.
  - In response to an official written request from the Gardaí on official Gardaí letterhead or email or other relevant authorities where provided for in applicable legislation.
  - In response to an account owner request that has been ticketed, reviewed and approved.
  - To maintain the operational integrity of the service (e.g. to detect phishing emails or abuse of the system or other security or technical issue).
  - To determine if there has been a violation of the NUI Galway ICT Regulations subject to the authorization of Director of ISS or a member of UMT in conjunction with a senior manager in ISS sign off.
  -

2. **For All Students** University IT resources are the property of NUI Galway and are to be used for legitimate purposes only. As an end-user of these systems, on completion of their course of study, students must ensure that they do not have the ability to gain unauthorised or inappropriate access to University resources because of access they had as a student within the University. If a student retain such access they should advise Information Solutions & Services (ISS) so that it can be removed.

3. IT Services provided to students

All registered students are provided with the following services to support their academic activity.

i. Email
ii. Personal productivity tools (currently the Office 365 product set)
iii. Online Storage
iv. Wi-Fi
v. Printing
vi. Computer Suites and associated software
vii. Library catalogue and databases
viii. Online Registration system
ix. The Virtual Learning Environment (Blackboard and associated software)

x. Exam timetable and results
xi. NUI Galway Apps

A full list of IT services provided by ISS are listed here.
Continued access to IT Services is subject to students complying with relevant University IT Security policies and is subject to QA616 NUI Galway Student Code of Conduct

4. Student Accounts Removal

Student accounts access (other than PHD students – i.e. undergraduate students and taught post-graduate students) will be disabled 180 days after the course end date.
In recognition of the need for PHD students to retain access to email/research data beyond the end of their programme of study, access to PHD student accounts will be removed 2 years after their course end date.
ISS reserves the right to disable inactive accounts where accounts have been inactive for a period > 90 days. The student can reactivate these accounts by contacting ISS. Inactive accounts will also be removed as per the timelines described above.

5. Student Accounts Data

Students are responsible for exporting data they wish to retain from their NUI Galway account in advance of the account closure date. NUI Galway does not provide any automated facilities for this.
Loss of data: While NUI Galway and its partners have procedures in place to manage data, the University does not accept any liability for loss of student data.
Destruction of Data: Data contained in Student accounts will be deleted in line with relevant data retention schedules as they relate to specific services and systems.

6. Auditing of Student Accounts Data and Access

Access to individual student account data and access logs is restricted to ISS technical staff and Library & IT service desk staff engaged in issue resolution and operational monitoring.
Data from access logs is used to support student retention analysis. Access to this data is defined in the DPIA (Data Processing Impact Assessment). A copy of this can be obtained by emailing issadmin@nuigalway.ie.

Deviation from this policy will require IT Security Committee approval.

5. Policy Responsibilities

Name	Responsibility
ÌCT Security Committee Chair	Policy Owner
Director ISS	Revisions and updates to the policy
ICT Security Committee	Approval of the Policy
All End-users (refer to end-user policies)	Responsible for implementation of policy.
ISS	Monitoring and reporting compliance with the policy

6. Related Documents

QA400 Data Protection Policy
QA433 ICT Regulations
QA411 End User Policy