



Code: QA434 Retired-Leavers-Movers Policy
Title: IT Policy for staff who Leave, Retire or Move departments
Date: 05/12/2017
Approval: University Management Team (UMT)

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 Access to the University's computing facilities is a privilege granted to members of the University which can be withdrawn. 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 when a member of staff retires, leaves or moves departments within the University.

2. Description

This policy applies to:

- All staff members who leave the University
- All staff members who retire from the University
- All staff members who move departments
- All third parties (External Account holders) who move between departments
- All line managers responsible for staff members and third parties (External Account holders) who have access to University IT Systems.

It is the responsibility of those staff types outlined above to read this and related security policies and be familiar with their contents.

It is the responsibility of line managers to ensure all staff using IT systems are aware of and understand their responsibilities in relation to this policy (and related policies) and to ensure any unrequired access is revoked when Staff Members retire, leave or move departments on a temporary or otherwise basis.

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 Galway employed or Agency employed or an External account holder within any area in NUI Galway.

“Line Manager” refers to any member of staff who is a line manager or person responsible for a member of staff.

4. Requirements

1. **For All Staff** - 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, when leaving, retiring or moving departments you must ensure that you do not have the ability to gain unauthorised or inappropriate access to University resources because of access you had in a previous position within the University. If you retain such access you should make your Line Manager and Information Solutions & Services (ISS) aware so that it can be removed.

Line Managers should ensure that additional IT access provided to a staff member specific to their job is removed when that staff member leaves the department.

2. For Staff Moving

When a staff member leaves a department or changes roles within a department, **the line manager** of that staff member in their previous role is required to request from ISS the removal of any IT access rights provided to that staff member which were specific to their previous role.

This is done through raising a Movers ticket with ISS Service Desk, which includes the employee staff identity number, and the detail of which specific access rights need to be changed – these should include, but are not limited to, any access rights currently held on Agresso, Quercus, Core HR and SharePoint sites and file-shares.

Staff who have moved roles within the University shall ensure that access rights to NUI Galway Systems have been revised in a timely manner appropriate to the new post they have taken, and report to ISS should they become aware that they retain access rights to systems which are no longer required in their new role.

3. For Staff Retiring

The University provides a continuing level of access to computing resources to retired staff as a benefit and courtesy. Retirees will retain indefinite access to their IT account to allow access to the following services subject to ongoing fair and reasonable usage:

- i. Email
- ii. Wi-Fi
- iii. General Access Computer Suites
- iv. Core Portal (HR) - retain the access to online review of pension or tax related details
- v. The Virtual Learning Environment (Blackboard)

The Library will additionally provide continuing access to their services to retired staff.

Other than as noted above, on receipt of notification of a retirement through the HR System, ISS shall through a combination of automatic and manual processes remove the retiree’s access rights to remaining centrally managed IT systems; the staff member will additionally be removed from the All-Staff email distribution list and added to the All Retired Staff distribution list.

The University recognises and values the ongoing contribution of retired staff who remain engaged in research, teaching and learning, and other core activities. These retirees may through sponsorship of a Head of Unit and application to ISS be provided with access to any additional services or applications required to perform those activities. In such cases, the Head of Unit is accountable for rights granted under this sponsorship and such access will be subject to regular review.

4. For Staff Leaving the University

Within five working days of receipt of notification from HR of a member of staff leaving the University, **ISS shall** remove that staff-members access to:

- a. The Financial Management System (Agresso)
- b. The Student Records System (Quercus)
- c. The Human Resources System (CORE HR)

Through automated process **ISS shall** ensure that staff leaving the University will have their primary Campus Account automatically disabled 120 days after leaving, and deleted after a further 365 days.

All Line Managers shall ensure that any requirement to remove or change the level and scope of IT access of a member of staff who has left the University which falls outside the standard processes as outlined above is made in a ticketed request to ISS. Such request must include the employee staff identity number, and the detail of which specific access rights need to be removed.

Deviation from this policy will require IT Security Committee approval.

5. Policy Responsibilities

| Name | Responsibility |
|--|---|
| ICT Security Committee Chair | Policy Owner |
| Director ISS | Revisions and updates to the policy |
| University Management Team | Approval of the Policy |
| All End-users (refer to end-user policies) | Responsible for implementation of policy. |
| Internal and external audit | Monitoring and reporting compliance with the policy |
| Line Managers | Notification to ISS of Movers, Leavers or any circumstance which requires a staff-member's level of access to systems to be changed other than as outlined above. |

6. Related Documents

QA400 Data Protection Policy
 QA401 Data Handling
 QA402 Data Classification

QA406 Remote Access Policy
QA408 Logical Access Policy
QA411 End User Policy
NUIG Retired Staff Policy