Maynooth University
IT Services

Maynooth University
Identity and Access Management Policy

Policy Details and Revision Record

Policy Name:	Identity and Access Management
Version Number:	1.5
Policy Owner:	Head of IT Operations
Approved by:	IT Services Management
Approval Date:	27th June 2022
Next Review Date:	Q2 2024

Appendix A - IDAM service matrix *(available by request to servicedesk@mu.ie)*

1. Policy Title

Identity and Access Management Policy

2. Policy Statement

This policy describes the approach and processes used to manage identities and access by IT Services to ICT services for users i.e. Maynooth University employees, students and third parties.

3. Policy Scope

The scope of this policy outlines

- the processes associated with the identity management system.

  (i) Creating a new identity
  (ii) Provisioning an identity to access ICT services
  (iii) Granting access rights for an identity for an ICT service
  (iv) Revoking access rights from an identity
  (v) Removing an identity

- How access to ICT services is administered to ensure that users have the appropriate level of access.

Physical access to University buildings and rooms is outside the scope of this policy but it is assumed that the identity management system may be used as a data source for an electronic access control system.

4. The Purpose of the Identity and Access Management Policy

The purpose of this policy is to ensure that identity and access management is undertaken in a manner that provides:

Confidentiality

(i) Ensuring that users have access to both their own personal data and ICT services required to undertake their studies or job/role.
(ii) Ensuring that each identity created is in compliance with University policies e.g. Password Policy

Integrity

(iii) Enabling the integration of data regarding user identities held in different systems.
(iv) Allowing users to authenticate to an ICT service using a username or other digital identifier and, where appropriate and secure, authenticates them automatically using single-sign-on.

Availability

(v) Minimising the overhead on the role of account/access administrators of individual ICT services and on users themselves.

5. Policy Principles

Identity Allocation

Wherever possible, an individual user will have a single identity for use across all ICT services.

This will not be the case where-

- A user is accessing ICT services in more than one capacity (e.g. they are an employee and a student), it may be necessary to create a secondary identity for that individual in addition to their primary identity.
- If privileged or administrative access is required, this may operate with a separate user account that is manually created by the IT administrator of a key business system and/or ICT service.

Identity Classification

The following classifies the different identity types:

(i) **Students** are typically eligible for registration, fully registered, or eligible for re-registration. The identity management system identifies registered and unregistered students.
(ii) **Employees** with a contract of employment.
(iii) **Affiliate** users are approved by a Head of Department. Affiliates are provided with similar access as staff to ICT services available to all employees e.g. Wi-Fi, Microsoft 365. Examples include external examiners, visiting lecturers and interns/work placement.
(iv) A contractor referred to as a **consultant.** A third party user requiring access to ICT services typically in a support capacity. No employee services are provided e.g. email.
(v) **Guest**. A temporary access to an ICT service. No employee services are provided e.g. email.

Single Sign-On and Multi Factor Authentication (MFA)

Single sign-on technology is used to allow a single authentication have access to multiple ICT services, e.g., a login to the Microsoft 365 Portal may allow automatic access to the Moodle VLE without the need to login again. Single sign-on may not be feasible for administrative access to key business systems as an administrator may have a second user identity for administrative access.

Multi-Factor authentication is implemented wherever appropriate and feasible and is required for remote/off-campus access to certain ICT services e.g. Microsoft 365.

Source Systems, Creating an Identity

The Student Information System is the single authoritative source of student data for the Identity Management system. Changes in student data, registration status and course enrolment data from the Student Records System will drive the identity management process.

The HR System is the single authoritative source of employee data for the Identity Management system. Starters, leavers and changes in staff data from the HR System will drive the identity management process.

Affiliates, Guests and Consultant identities are created on request and approved by Head of Department or appropriate authority.

Access Rights – Provisioning an Identity

Access rights are expressed as the ability to access/login an ICT service, a privilege level within a system or as access to particular elements of the system

Standard access rights are provided to all users as outlined in Appendix A.

Access Management - Granting, Revoking & Reviewing

Users will be provisioned to use systems and given access rights required to undertake their individual job or role at the University. It is recognised that during a period of employment, an employee's role may change and therefore their access rights will need to be modified accordingly.

Access rights to key business systems are approved by and reviewed regularly with the Head of the Business unit or appropriate authority. Access rights will be revoked on request of the Head of the relevant Business unit or appropriate authority.

Privileged access to ICT services e.g. Office365, servers, databases etc. are approved and reviewed regularly with the IT Head of Function or appropriate authority. Privileged access rights will be revoked on request of the IT Head of Function or appropriate authority.

Joiners, Leavers & Removing an Identity

Joiners

The Identity Management system is dependent on the quality of data from its source systems and the timeliness of data updates ensure that every user has the appropriate access rights at the correct time. Identities and basic access rights for employees and students will be created within 24 hours of the data being available in the source system and that individual being in a status eligible for an identity to be created.

Leavers

The de-provisioning of employee and student identities and associated access to ICT services is a semi-automated, managed procedure, to prevent accidental deletions.

Employee and student identities will be revoked within 6 weeks of an individual no longer being eligible. The leavers process for employees is a batch process and operates on a regular basis as required. Student leavers operates annually with student identities provided through to graduation.

Affiliate accounts are set to expire either on the date provided by the approver to a maximum of 1 year after creation. Consultant accounts are set to expire on the date provided.

6. Roles and Responsibilities

6.1. Business Units – Registry, HR

As the source systems for the Identity Management System, it is the responsibility of the Human Resources and Registry units to ensure that a high degree of data quality is maintained and that the system that holds that data is updated in a timely fashion.

6.2. Heads of Department

Approve affiliates, access to key systems and privileged access to ICT services as appropriate.

6.3. IT Services

Operate the identity management system and access processes

7. Definitions

Access rights or **permissions** are used to control who can do what in a given system or service. The 'who' is specified in the form of a single identity or set of identities (a group) and the 'what' is defined as a set of permissions e.g. read-only, create, edit, delete. Access rights can be granted (added) or revoked (removed).

Authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources/data in an information service or system.

Authoritative Source
Defined as the service that is the system of record and data for a particular type of user, e.g., the Student Information System is the authoritative source for all students.

ICT Services
MU systems/services that are accessed from the network. These include information systems, website and teaching & learning systems.

Identity is defined as a means of identifying an individual through electronic means usually in the form of a username.

Identity Management system
Defined as the system that accepts data for students, staff members and affiliates from the appropriate source systems and using predefined business rules, creates identity accounts and provisions those accounts to access a variety of University systems according to those business rules.

Key Systems – Key systems are services that support VLE, Financial, Student Administration and HR.

Provisioning is defined as activating an identity to use a particular system or service with de-provisioning deactivating access from a system or service for an individual.

Users
A **student** is defined as a person who is going to be, currently is or has been registered at the University as a learner.
A **staff member** is defined as a person who is employed and paid by the University.
An **affiliate** is defined as a person who requires electronic access to University systems/services but who is not classified as a student or staff member, and is not paid by the University in any capacity.
A **consultant** is defined as a third party user requiring access to ICT services typically in a support capacity. No employee services are provided e.g. email.
A **guest** is defined as a person who requires temporary access to an ICT service. No employee services are provided e.g. email.

Single sign-on is a technology used to allow a single authentication to permit access to multiple systems without the need to login to each system individually, thus saving the user time.

8. Relevant Information

Related Policies

Maynooth University Password Policy
Maynooth University Information Security Policy

Supporting Processes

Student Account Deletion Process
Staff Leaver Process

Version History

Version	Date	Author/Editor	Comments
1.0	18/2/2020	Peter Gaughran	Initial draft
1.1	17/7/2020	HEAnet	Review and comments included
1.2	19/4/2021	Peter Gaughran	Additions regarding leavers, affiliates
1.3	26/4/2021	Peter Gaughran Joanne Madden	Additional reference documentation
1.4	June 2022	D O'Reilly	Further review and formatting to align with IT Services policy template.
1.5	June 2022	D O'Reilly	Edits to incorporate final feedback

Maynooth University
IT Services
Maynooth, Co. Kildare, Ireland.

Seirbhísí TF
Ollscoil Mhá Nuad
Maigh Nuad, Co. Chill Dara, Éire

T +353 1 708 3388 **E** servicedesk@mu.ie **W** maynoothuniversity.ie