



Ollscoil Chathair  
Bhaile Átha Cliath  
Dublin City University

## **Digital Identity**

## **Retention Policy**



## Table of Contents

Introduction .....	2
Purpose .....	2
Scope .....	2
Policy Statement .....	3
Roles & Responsibilities .....	5
Definitions .....	5
Related Documentation .....	5
Contact .....	5
Policy Review .....	6
Version Control .....	6

## Introduction

The possession of a dcu.ie identity is generally taken by the outside world to mean that an individual is “at” DCU (Dublin City University & hereinafter referred to as the ‘University’) and assumptions may be made about an individual’s formal relationship with the University.

In addition, an individual’s dcu.ie identity also acts as a passport to gain access to certain digital systems and services, both within and outside the University.

Regulating access to a dcu.ie identity is important for the following reasons:

### **Cyber security**

Cyber security is a growing concern for the University, as a serious cyber-attack has the potential to cause severe and costly disruption to the University’s operations.

### **Data Protection**

Under GDPR legislation, as a Data Controller, the University has a duty to protect the personal data within its possession, including the data of staff, students, research participants and others. In addition, one of the principles of data protection law is that personal data may only be retained for so long as there is a business purpose or case for doing so and therefore one of the effects of this policy will be to regulate how long personal data within certain IT systems, like the email system, will be retained.

### **External Relationships**

The University is being increasingly required by various external partners (e.g. research funders, accreditation bodies etc.) to demonstrate that it has effective policies, procedures and controls in place to protect systems and data.

### **Reputation Management**

The dcu.ie domain is a key part of the University’s brand and anything that happens in that digital domain, could impact upon the University’s reputation.

## Purpose

The purpose of this policy is to establish who gains access to a dcu.ie digital identity and for how long they may retain that access.

## Scope

This policy applies to:

- a) all units of the University (both academic and professional), including its subsidiary campus companies and research centres, which are all hereinafter collectively referred to as either the ‘University’ or ‘DCU.’

- b) all current employees of the University who are eligible for a dcu.ie digital identity.
- c) all registered students of the University who are eligible for a dcu.ie digital identity.
- d) all other parties (e.g. Emeritus title holders, Members of Governing Authority, Agents, Contractors, Visitors etc) operating both within a DCU campus and on behalf of DCU who are eligible for a dcu.ie digital identity.

## **Policy Statement**

### **Eligibility for a dcu.ie digital identity**

#### **Route A: Automatic Eligibility**

Individuals can be eligible through a formal relationship with the University. Eligibility in this category will last as long as the formal relationship or title lasts. This category consists of:

- Current employees of the University, including employees of wholly owned subsidiaries of the University.
- DCU Students
- Current members of the Governing Authority
- Retired members of staff who have been awarded an emeritus title in line with the DCU Emeritus Staff Policy.

#### **Route B: Sponsored Eligibility**

##### ***Sponsored accounts***

Individuals may be eligible for a sponsored account.

An application for a sponsored account should be sponsored by the relevant Head of Unit and approved by the relevant member of the Senior Management Group (SMG).

##### ***What is a sponsored account?***

A sponsored account gives the holder access to DCU's systems.

Access permissions to enter physical locations (e.g. swipe access for buildings or rooms) are outside the scope of this policy, which is limited to the granting and retaining of DCU digital identities.

## **Who is eligible?**

Requests for sponsored accounts are assessed on a case-by-case basis. Any application for a sponsored account must adequately demonstrate the need for such an account.

Note: anyone who has an active contract of employment with the university does not require a sponsored account, a DCU account and access to relevant systems is provided as part of their terms of employment.

## **How to apply**

All applications should be made through the Request for a Sponsored Account form.

Sponsored digital identities will be valid for a maximum period of one year; after which time, the sponsor will need to reaffirm sponsorship and the need for the account to be retained for up to another twelve months. This must also be reapproved by the relevant member of SMG.

Sponsored digital identities may be revoked at any time by the relevant Head of Unit, a Member of the Senior Management or the Director of Information Systems Services.

## **Digital Identity Eligibility**

The following table summarises eligibility for a dcu.ie digital identity and the period after which associated account data will be deleted.

### **Summary**

	<b>Digital Identity Eligibility Period</b>	<b>Grace Period (beyond eligibility period)</b>	<b>Account and Data Deleted</b>
Current DCU employees	Duration of employment contract	None	At the end of the eligibility period*
Sponsored digital identities (contractors, visitors, etc)	Maximum of 1 year subject to renewal of sponsorship	None	At the end of the eligibility period
Emeritus title holders	Duration of title	None	At the end of the eligibility period
DCU Students	Duration of student registration	Until 1 <sup>st</sup> October of the year following Graduation	At the end of the grace period

	Digital Identity Eligibility Period	Grace Period (beyond eligibility period)	Account and Data Deleted
Current members of the Governing Authority	Duration of membership	None	At the end of the eligibility period

\*Retired staff will retain authentication access to the CoreHR system for access to pension data. All existing retired staff will receive 90 days' notice before enforcement of this policy.

### Account Suspension

Under certain circumstances, a digital identity may be suspended with immediate effect.

## Roles & Responsibilities

Staff, students, visitors and others associated with the University have a responsibility to ensure that their actions comply with both the requirements and the spirit of this policy.

Heads of Schools and Units are responsible for ensuring the implementation of the policy in relation to the activities of their departments.

The Director of ISS has overall delegated responsibility for coordinating the implementation and the day-to-day operation of the policy.

## Definitions

dcu.ie digital identity	This is defined as the unique identifier of a user on all dcu.ie domains and all associated stored data.
-------------------------	--

## Related Documentation

This policy should be read in conjunction with other [University ICT policies](#).

## Contact


Further clarification on this policy can be sought from the Director of Information Systems Services (ISS).

## Policy Review

This policy will be reviewed as and when changes are required. The Director of Information Systems Services (ISS) will draft the necessary changes and have them reviewed and approved in advance by the IS Governance Committee as appropriate.

Anyone in the University can determine the need for a modification to the existing policy. Recommendations for changes to this Policy should be communicated to the Director of ISS.

## Version Control

<b>Document Name</b>	Digital Identity Retention Policy		 Ollscoil Chathair Bhaile Átha Cliath Dublin City University
<b>Unit Owner</b>	Information Systems Services (ISS)		
<b>Version Reference</b>	<b>Original Version 1.0</b>	<b>Reviewed Version 1.1</b>	
<b>Approved by</b>	Executive	Executive	
<b>Date</b>	28 <sup>th</sup> November 2023	28 <sup>th</sup> June 2024	

End.