UCD IT Services

IT Account and Service Access Procedures

Purpose

University College Dublin (UCD) provides information technology (IT) services to its users in order to perform work for the University in support of its mission. In order to access these services users require an IT Account. UCD IT Services provides users access to central IT services, support and infrastructure and this document outlines users eligibility for and entitlement to these services.

The University's Acceptable Use policy governs user's access to and use of the IT Account and services and by use of the IT Account and services a user is indicating acceptance of the University's Acceptable Use Policy. This document is supplemented by, and should be read in conjunction with, the University's Acceptable Use Policy.

1. Definitions

A **Service** is an IT service or application delivered by UCD IT Services.

A **User** is any person, with a recognised requirement to do so, using a service provided by UCD IT Services.

A **Customer Category** is a high level indication of the role of the user.

An **Entitlement** is access to a service based on the privilege of the account as determined by the customer category/role of the user.

An **IT Account** is an authorised user account, provided for the purposes of accessing services as granted by entitlements to that user account. UCD retains ownership of all data and services arising from accounts issued by UCD.

An **Account Holder** is an authorised user with data that is stored on a University supported IT service or University owned device.

The University's **IDMS** (identity management system) derives and records entitlements to IT services for all users.

SISWeb is the University's system to provide student access to the student record system.

Multi Factor Authentication (MFA) adds an additional layer of protection to non-student IT accounts and helps secure and protect both personal and the University's data and reputation.

The **Account Status** of an IT account may be :

- Enabled (Account holder can access services)
- Disabled (Record and associated data remains in UCD authentication services but account holder cannot access services). UCD IT Services may provide temporary access to a disabled account to the account holder in accordance with a request being authorised by the Data Protection Office. (See the Data Request Policy and form)

- Deleted (Record and associated data is removed from UCD authentication services). IT accounts will be deleted one year after they are disabled.

A **Sponsor** is a UCD staff member who requests access to service on behalf of another individual (a visitor).

An **Approver** is an individual (typically a Head of School or Unit) suitably authorised to approve a request for access to service.

2. Scope

This document applies to all users with enabled IT accounts for the Customer Categories outlined below.

In order to qualify for services, a record must be designated "Active"[1].

Customer Category	Who does this include?
Staff	• Staff members • Prospective staff • Retired staff with post-retirement contract • Emeritus RTA
Non Contractual Appointees	• Non-Contractual Appointees
Student	• Registered students of the University
Direct Applicant	• Direct applicant to the University
Hourly-paid Persons	• Casual / hourly claimants • Stuworking* Retain student account
Sponsored IT accounts (eligible Visitor / Affiliate record types)	• Research collaborators • Staff of recognised colleges • Temporary or affiliate admin or professional • UCD Foundation staff • Visiting academic / researcher • Other eligible record types
Retired staff	• Pensioners
Alumni	• Alumni
Non Person	• Email Only • UCD Foundation • Centre for BioNano Interactions (CBNI) • Conference Accounts

The entitlements of different customer categories to services are detailed in the accompanying *Service Entitlement Matrix.*

[1] Alumni are the exception. They are designated in IDMS as "Inactive Alumnus"

3. Procedures

IT Account (and the services thereof) eligibility

- **Staff** members become eligible for an IT account as soon as their record becomes active in the University's HR system. The steps that should be taken by an incoming staff member to ensure that their HR record is active in a timely manner are outlined in HR onboarding information.
- **Students** applying through the CAO become eligible for a full IT account within three days of accepting a place in University College Dublin.
- **Direct applicants** are eligible for a basic IT account when applying but will only be assigned the role of "Student" once they progress their registration.
- **Hourly Paid Persons** become eligible for an IT account as soon as their record becomes active in the University's HR system.
- **Sponsored IT account holders** become eligible for an IT account once a suitably authorised person (the approver) adds them to the University's identity management system. The approver can initiate an entitlement to information technology services. The resulting IT account will remain active for a fixed period (maximum of one year). *Sponsored IT Accounts issued to individuals who subsequently attain a different role (become staff, for example) cannot be converted to a different account type. A distinct IT account will be issued to the individual in this case.*
- **Retired staff who retire as UCD staff** On the account holder's retirement date their role will be converted to retired staff and the resulting changes to service entitlements will be effected immediately.
- **Retired staff who resign from UCD and subsequently retire** IT accounts for this category of account holder will be disabled and deleted. A new account for such customers will be available on request.
- **Alumni** Graduating students will have their customer category on their existing IT account converted to alumni. This will happen automatically on the last day recorded in SISWeb of the academic year in which they completed their programme of study.
- **Non-person Accounts** A non-person account will be created by the IT Helpdesk on receipt of a written request (which includes a personnel number) from a UCD staff member (the sponsor). Non-person accounts are created for a fixed period (maximum of one year). It is the responsibility of the sponsor to monitor email correspondence to the account.

Note: All non-student accounts are protected by **Multi Factor Authentication (MFA)** as standard. It is a mandatory requirement for all non-student users to enroll in MFA at the time of account set up.

Non-student users are also required to install a small security application on any device connecting to University IT resources as part of **Multi Factor Authentication (MFA)** enrollment. This application checks that the device meets the security standards as set out in the Device Protection Policy. Provided the device meets this policy, access to University systems is allowed.

IT Account (and the services thereof) removal

- **Staff**
  - ***End of Contract*** The IT account of a staff member will become disabled 30 days after termination of their employment with UCD. Approximately one month before the termination of employment (where the date of termination is known), the account holder will be notified through available mechanisms.
  - ***Career Breaks*** A staff member on a career break of less than one year is entitled to retain access to their IT account and resulting services. For staff members on a career break of longer than one year, there is no retention of user accounts or provisioned services. The IT account will be disabled as above and deleted one year thereafter. On return, a new user account is issued. (See Section 4.7 of Career Break Policy)
- **Students**
  - ***Students who graduate*** Alumni retain access to basic IT services to allow access to transcripts.

- ***Students who commence but do not complete a programme*** In respect of students who commence a programme of study but do not complete it, access to all services will cease 180 days from the last date of registration in the student registration system, at which time the IT account will be disabled.
- ***Students who accept a place but do not commence a programme*** Students who accept a place in University College Dublin but do not complete their registration and commence a programme of study will have their IT account deleted 15 - 30 days from cancellation of their registration in the student registration system.
- ***Direct Applicants who do not progress with their application*** Applicant accounts will disable and delete 15-30 days after no longer being an active applicant in the student registration system

- **Hourly Paid Persons** The IT account of an hourly paid person will become disabled upon termination of their employment with UCD. Approximately one month before the account is disabled (where the date of termination is known), the account holder will be notified through available mechanisms.
- **Sponsored IT accounts** 30 days before the date of account closure, both the account holder and the Sponsor will be notified using available mechanisms. At this point, the account can be renewed for a further fixed period by the Sponsor. If the employment of a Sponsor of an account terminates, the account holder will be provided with two weeks' notice of closure. The account can, during this period, be renewed by an alternative Sponsor.
- **Retired staff and Alumni** IT accounts are disabled upon the death of the account holder.
- **Non-person accounts** 30 days before the expiry of the account, an email will be sent to both the email address of the account and of the account sponsor advising of the pending closure of the account and offering the option to renew the account for a further period. If the account is not renewed, access to services will cease on the expiry date for the account. At this time the account will become disabled. If the employment of the sponsor of a non-person account is terminated, an email will be sent to the account holder providing two weeks' notice of closure. The account can, during the notice period, be renewed by an alternative sponsor.

Exception

- UCD IT Services may withdraw service access from any user arising from a suspected breach of University policy; or where a security incident is suspected, or in the event of an authorised request from a University or external regulatory authority. In this event, the user shall be notified via available mechanisms, which may include notification to their Unit, Sponsor, School or programme administration. Withdrawal of access shall be for a period of time to be determined by UCD IT Services as necessary to assess or remediate any incident, and return of service access may be contingent on the completion of a University disciplinary or external regulatory process. Service may be permanently withdrawn by UCD IT Services, on behalf of the University, arising from such a process.

4. Roles & Responsibilities

The University is responsible for:

- The provision of identities for staff and students in a timely manner
- Deprovisioning of staff and student records in a timely manner

Account holders are responsible for:

- Complying with the Acceptable Use Policy
- Complying with the University's Password Protection Policy
- Complying with the Device Protection Policy

Approvers are responsible for:

- Ensuring that requests for access to services are authorised only where such access is required for the normal conduct of University business

Sponsors are responsible for:

- Full lifecycle management (creation, renewal, removal) of all IT accounts that they sponsor
- Ensuring that the holders of accounts sponsored by them are familiar with the Acceptable Use Policy and the Password Protection Policy and Device Protection Policy

5. Related documents

- Service Entitlement Matrix.
- Acceptable Use Policy.
- Password Protection Policy.
- Data Request Policy.
- Career Break Policy.
- Device Protection Policy

Version history

- V1.0 Initial draft – ITLG February 2019
- V2.0 Final Draft - Core IDMS Group September 2019
- V3.0 Final edition for publication - 14 February 2020
- V4.0 Amendment to include MFA - 12 January 2021
- V4.1 Amendment to update URL and Section numbering - 17 November 2021
- V5.0 Amendment to date of staff IT account closure - 9 February 2022
- V.5.1 Amendment to reference section of Career Break policy - 12 September 2022
- V6.0 Amendment to Alumni section - 12 September 2022
- v7.0 Amendment to include Direct Applicants account provisioning - 4 Jul 31, 2023
- v8.0 Amendment to Students not completing programme; adjustment to Alumni section; inclusion of Device Protection Policy; addendum to Multifactor Authentication section for device check application - April 2024