Policy

University IT Account Entitlement and Rights Assignment Policy

Last updated: 12/05/2026

Version control

Version number	UEB Sponsor	Approval Body/Officer	Date of approval
V2.3	Chief Digital and Information Officer	Senior Information Risk Officer	16 March 2026

For queries on this policy please contact:

IT Support:

- email: **it-support@cardiff.ac.uk**
- tel: 02922 511111 (ext. 11111 internally)

Purpose and scope

The purpose of the policy is to set out the principles upon which decision shall be made in respect of the creation, management, suspension, and deletion of a University IT account.

This policy applies to all IT accounts that are created and hosted by Cardiff University IT, and to externally created or hosted accounts that seek permission to connect to the University's IT network, IT Systems and services, or other IT Systems and services associated with Cardiff University.

Breaches of this policy may be treated as a disciplinary matter and dealt with under the university's staff disciplinary policies or the Student Conduct Regulations as appropriate.

Related policies and procedures

This policy forms part of the Information Security Management Framework. It should be read in conjunction Information Security Systems Controls Policy and all supporting policies.

Policy

1. The creation, management, suspension, and deletion of IT accounts shall be managed in accordance with overarching principles which ensure that the University's resources are used effectively, that its legal obligations are complied with, and that its information assets are appropriately protected in terms of confidentiality, integrity, and availability.

2. IT accounts shall only be created when a user falls within one or more entitlement category as determined and published by the University Membership Categories and Entitlements Group (MCE). Any individual exceptions to this shall be approved by the Chair of the Information Security Oversight Group (ISOG). The MCE group will consider if exceptions require an additional Category, which will in turn be approved by ISOG.

3. When determining entitlements, the MCE shall take into consideration how the entitlement (or modification or withdrawal of entitlement) supports the University's strategic goals, the effective use of resources, compliance with legislative and contractual obligations, and the risks to security of information assets in terms of confidentiality, integrity, and availability.

4. Access granted shall be in line with the person's role and applied on the basis of least

privilege, and access shall be removed when no longer required. Access requests shall be approved by the relevant Business Owner, Information Asset Owner, line manager, or IT Rights Authority Holder.

5. Any enhanced/privileged access shall be applied to a separate service account attached to the owner's identity. Service account requests will be approved by the line manager or relevant Business Owner. Service accounts should be limited to use for the enhanced access only and not duplicate access that has been granted on the primary account, such as email. Service accounts shall be reviewed annually to ensure the rights applied to them are still appropriate to the role. Service accounts will be closed down immediately after the owner leaves the University.

6. IT account creation and management shall be automated and managed via a single identity management system as far as feasible to ensure efficient operation. Where powers to create and manage accounts for entitled groups or individuals are devolved, those powers should only be used where it is:
   - not possible to use the existing data authority systems (Student Records Systems, HR system) to feed the central identity management system as the user does not fall within the appropriate category or;
   - not operationally practicable to use the existing data authority systems for other reasons which are in the University's best interests.

All account creation and management, whether centrally or locally conducted, shall comply with this policy and the MCE tables.

7. The authoritative data source for determining each membership status shall be defined by the University IT Service and processes and procedures shall be established in liaison with Human Resources, Admissions, and Registry to ensure that staff**,** student and applicant accounts are suspended and deleted at the appropriate point following a change of status.

8. IT system access for non-members shall only be granted on completion of an IT Access Request form by a Sponsor and approval from the relevant IT Rights Authority Holder. The Identity Management and Entitlements team will review all requests to ensure they align with the MCE policy before creating accounts or granting access to any IT systems. No accounts for non-members will be created for a period of more than 1 year. Extensions to the expiry date may be granted on request, and with approval of the Sponsor or IT Rights Authority Holder.

9. IT accounts shall be managed during their lifecycle and shall be suspended or deleted in accordance with MCE such that when the status of the user changes there are safeguards in place to ensure that the entitlements remain appropriate or are removed at the appropriate point.
   1. Staff accounts will be closed within 24 hours of contract end, unless the individual transitions to a new role or MCE category, in which case access rights will be reviewed and adjusted.
   2. Student accounts will be closed 90 days after their student record has been closed down in the student records system, unless they are confirmed to have moved to another category, whereby access rights will be reviewed and amended accordingly.
   3. Non-member accounts will be closed down on the expiry date specified at the time the account was requested. Extensions to the account must be approved by the sponsor or IT Rights Authority Holder, who will confirm that the access rights remain appropriate to the role. Accounts will not be extended for more than 1 year at a time.

10. Staff and students shall be given appropriate notice of the impending routine closure of their account. For staff this will be at least 1 months' notice (where the member of staff's contractual notice period is in excess of a month) and for students this will be at least 3 months' notice. Communications shall be embedded into existing leavers processes.

11. No notice period is prescribed where accounts are suspended for reasons other than routine closure.

12. When designing authentication mechanisms to allow access to University IT resources and applications, the mechanism design should ensure that the basis for authentication reflects the relevant entitlement as set out in the MCE. Where a technical solution is not possible the risk of proceedingdifferently should be signed off by the Business Owner. Design of access and authentication mechanisms should also comply with the Information Security System Controls policy.

13. Users shall be given a predefined set of rights and entitlements which shall reflect their membership category entitlement as per the MCE. Where specific authorised roles require additional rights, these will be maintained in the central Identity Management System with an appropriate audit trail of authorisation. Access granted to any individual should be in accordance with the needs of their role and based on the principle of least privilege.

14. Users shall be given a unique username and email address. This is to be enforced by the identity management system. Permanent retention of skeleton user records is required in order

to ensure all usernames and email addresses are unique for all users who have a full account. Applicants who fail tobecome students are fully deleted every year.

15. Training requirements in relation to high and medium risk specific authorised roles shall be identified by Business Owners and University IT shall ensure that appropriate mechanisms exist to convey an individual's responsibilities in relation to 'enhanced rights' and to capture the agreement to comply with relevant policies.

16. Suitable feedback mechanisms shall be in place to ensure that when the holders of specific authorised roles change, the users' entitlements are appropriately amended.

17. Wherever possible an identity should have a single login account with as few accounts as practical per identity. Each login account is to be used by the individual specified in the Identity only. The use of shared 'generic' accounts is not permitted without a risk assessment and exception signoff by ISOG. Where privileged access to IT systems is required, such access rights may be delegated to an individually attributed service account to provide clear separation of role. For example:
    1. Where an individual has access to confidential university data that is not part of their substantive role (such as a Taught postgraduate working part-time in Registry), that access should be facilitated through clear separation of login accounts and identities.
    2. Where an individual has more than one contractual role, their title displayed in the email address book shall default to their largest contracted FTE role (such as 0.8 School of Engineering, 0.2 School of Mathematics, would default to School of Engineering). Exceptions may be addressed through local Human Resources.
    3. If the nature of an individual's relationship with the university changes, for example, a full-time member of staff becomes a full-time student, depending on risk, the established account may be deprecated in favour of a new account for clear separation of responsibilities and duties.

Other cases may arise that require a second account. These will be dealt with via the MCE group.

18. A review of accounts and access rights will be carried out annually by the Identity Management Team. Regular exceptions reports will identify accounts that have fallen outside of the criteria specified in this policy so that manual correction can be applied, or processes amended where a more widespread issue is identified.

Roles and responsibilities

The Senior Information Risk Owner is the sponsor for this policy, and responsible for approving the need to develop or substantively amend the policy, for presenting the final draft to the approving body, and for ensuring that their policy-making documents comply with, are monitored by, and reviewed in line with the Cardiff University Policy for the Development of Policy-making Documents.

ISOG is responsible for ensuring that the governance of the MCE is fit for purpose, including designating a Chair (it is noted that the Group's remit also covers University library entitlements). ISOG is also responsible for approving any exceptions to the MCE approved categories and entitlements.

The Chief Digital and Information Officer is responsible for ensuring that appropriate processes and procedures are established to support this policy. They are also responsible for authorising any exceptions that fall outside of the MCE entitlements. Any exceptions granted will be reviewed annually.

Business owners are responsible for ensuring that any authoritative data sources required for IT account identity management purposes are kept up to date and remain fit for purpose. This includes any Applicant and Student data on student record systems and Staff data on the HR system. Any changes to data structures or processes that impact data used for identity and access management must be communicated to the Identity Management Team via the HR Operations Group or the Student Systems Oversight Group. Information Asset Owners for student, applicant and staff data will be responsible for providing assistance to University IT in the development of their processes and procedures in accordance with point 7 above.

Business owners are responsible for ensuring that appropriate processes are in place for granting and removal of local access to their systems, as specified in the Information Security Specification (Systems Level) Policy.

The MCE Group is responsible for ensuring that a summary of categories and associated entitlements is published and maintained.

IT Rights Authority Holders are responsible for ensuring that requests for access for users who are neither staff nor students (such as contractors, temporary staff, research collaborators, and academic visitors) are appropriate, justified, fall within one of the approved categories, and that

any changes to users' circumstances impacting on their access entitlement are notified to University IT immediately.

Monitoring and review

This policy shall be reviewed every three years, at minimum.

Periodic reporting of Account & Entitlement statistics and trends shall be presented to ISOG.