Document Reference Number	UoG/ILS/IS 008
Title	Policy for User Account and Access Management
Owning Department	Information and Library Services
Version	4.5
Approved Date	10/12/2024
Approving Body	IT Management Board (IM)
Review Date	09/12/2025
Classification	Internal – Confidential

Version Control

Version	Last Modified	Last Modified By	Document Changes
4.5	10/12/2024	Atif Siddique	Section 4.1.6 updated
4.4	24/07/2024	Atif Siddique	Annual review. Minor grammatical updates.

Policy for User Account and Access Management

1.0 Purpose

1.1 The purpose of this policy is to set out the expectations for creating and managing university user accounts and access requests to the university's information resources.

2.0 Scope

2.1 This policy applies to all members of staff, students, researchers and third parties working in partnership with the university.

2.2 The policy applies to all university user accounts, access to network drives and shared folders, and access to other university IT systems (on-premise or in the cloud).

2.3 This policy applies to the following types of accounts and access:

- Standard user accounts – staff and students
- Affiliate accounts
- Privileged accounts including 'S' accounts, cloud administration accounts and system administration accounts
- 'W' accounts (local admin rights on desktops and managed laptops)
- Access to shared drives and restricted folders
- Generic accounts (network and email)
- Summer school/open day and visitor temporary desktop accounts
- Emergency access (breakglass) accounts
- Accounts for non-widely used IT systems/services: IT systems designed for use for specific job functions e.g. Finance and procurement, Student Record, HR, IT Service Desk and Library Management systems, etc.
- Delegate mailbox access
- Visitor wireless access
- O365 access

2.4 University faculties and directorates should ensure adequate controls are in place for user accounts and third-party systems (including social media platforms) that they operate and manage locally, and Information and Library Services should have governance over the controls implemented for these systems.

3.0 Reference to International Organisation for Standardisation (ISO) 27001

3.1 This policy complies with the university's information security strategy and draws upon the ISO 27002 Code of Practice.

4.0 Account and Access Creation and Deactivation

4.1 **Standard user accounts (staff and students):** are created via the Identity Management System. At the end of a staff member's employment or a student's exit from the university, the following will apply:

4.1.1 A staff account will be deactivated based on the end date of the contract or employment. However, data held in the account will be retained by the university after employment for 180 days after which it will be deleted. A deceased staff member's account will be deactivated upon notification.

4.1.2 Access request by an exited staff member to their files or email will be assessed on a case-by-case basis and may only be granted when there is a valid or acceptable reason for the request, and after authorisation by the relevant former line manager and/or head of department. Only a one-time request may be granted, and it may be supervised. In all cases, before granting access, the requester will be asked to provide answers to the security questions associated with the account. Any access request after the 180-day retention period will not be possible.

4.1.3 Reactivation of a staff member's account after the end of their contract or employment to complete a project or work relating to the university must follow a formal approval from the relevant authoriser for the department. Access may be granted for up to two weeks, and where access is required for more than two weeks, an affiliate account must be requested and approved by the relevant authoriser.

4.1.4 Any access request by a current staff member to an account belonging to an exited staff member may be granted for a short period depending on the business need, following a written authorisation from the relevant head of department. If necessary, the IT Service Desk may also notify the relevant senior member of the faculty or directorate for further authorisation. Where it is determined that granting access to the requester would conflict with interest, the request will be declined.

4.1.5 A student account will be deactivated based on the student's final result. That is, access to all university IT and Library systems will cease after 90 days from the "date of decision" after which any data maintained by the student (including email, Moodle, Portal, home areas) will no longer be accessible. 90 days will also apply to students with unsuccessful results. Where a student withdraws or is excluded, the account will be deactivated immediately. A deceased student's account will be deactivated upon notification.

4.1.6 Access requests to university IT and Library systems by an exited student after the 90 days (as explained in the section above) will not be granted.

4.1.7 All students employed by the university will be given a staff (JobShop) account. Account owners must ensure their staff accounts are operated solely for the intended purposes and separately from their standard student accounts. Line managers should ensure this is complied with during a student's employment.

4.2 **Affiliate accounts**: Individuals who work with the university but are not members of staff of the university, such as contractors, staff from partner colleges, and visiting academics will be given affiliate accounts. A start and end date will be assigned to an affiliate account to ensure access is deactivated automatically. The duration of an affiliate account will depend on the affiliate account type and the required period specified by the requester and authoriser. If the account is required beyond the end date, an extension will need to be approved. Affiliate accounts must be assigned access permissions commensurate with the business need. For example, where an affiliate account does not require university Portal access, email account or access to the network drives, such access rights must not be provided.

4.2.1 Affiliate account approvers in faculties and directorates must manage the affiliate accounts they approve in compliance with this policy including deactivation of the accounts when no longer needed.

4.3 **Privileged accounts (including 'S' accounts, cloud administration accounts and system administration accounts)**: A privileged account will have its unique username and password assigned to the authorised user following a formal request by the line manager or a designated staff member. A user must not elevate their access within their environment. Line managers or designated staff members must ensure privileged access is removed for staff members transferring from their departments to other teams or departments within the university. Privileged accounts must be reviewed quarterly to ensure they remain fit for purpose, withdrawn where no longer required, and must be sufficiently auditable. A privileged account must be operated solely for the intended purposes and separately from the standard user account.

4.3.1 Default privileged account passwords must be changed before any system goes live.

4.4 **'W' accounts (local admin rights on desktops and managed devices):** For specific business needs, W accounts may be granted for managed devices following approval by ILS. Where ILS determines that there is an alternative arrangement to a W account that will support the stated business need, the IT Service Desk will advise the requester of the alternative arrangement, and the W account will not be granted. 'W' accounts must be reviewed quarterly to ensure they remain fit for purpose, withdrawn where no longer required, and must be sufficiently auditable A privileged account must be operated solely for the intended purposes and separately from the standard user account.

4.5 **Access to Shared drives and restricted folders:** Access requests to a shared drive area and restricted folders that are not provisioned by default (e.g. belonging to a different department) will only be granted following approval from the relevant authoriser and only to the specific shared drive area or the restricted folder required. Owners should be cognizant that by authorising access for a user, confidential data present in their shared drive areas or restricted folders may become accessible to the requester.

4.6 **Generic accounts (network and email):** Generic accounts will be created where the use of a standard user account is not feasible to support a business need. The

requester must state the business need when requesting a generic account, and the account will be created following approval by ILS. An approved generic network or email account must have an owner (the requester or a designated staff member) and delegated access requests to a generic network or email account must be authorised by the account owner. Generic network accounts must have expiry dates assigned and must be reviewed periodically to determine if they are still required, where practical.

4.7 **Summer school/open day and visitor temporary desktop accounts:** The use of temporary desktop accounts will be kept to a minimal and shall only be issued where a request is sent to the IT Service Desk and approved by the relevant authorisers. Temporary desktop accounts shall remain inactive until they are requested for use and approved. Where possible, a named user shall be assigned to the account for the duration of its use, along with an expiry date. The account requester shall be responsible for ensuring account credentials are not shared beyond the user to whom the account has been assigned. A log of the account users must be kept and may be requested for review by the IT Service Desk for investigatory purposes.

4.8 **Emergency Access (breakglass) Accounts:** Some university systems may require the use of emergency access accounts to allow for access to the system in emergency scenarios where access would otherwise not be possible. Where an emergency access account is required, the request must be reviewed and approved by the Executive Director and Chief Information Officer or a nominee and should be added to a register for auditing purposes. Where an account is approved, appropriate measures should be in place to ensure it is secured. This includes the use of MFA where possible, a strong password with strict lockout rules and alerting to notify when the account has been used. Alerts must be sent to the Associate Director – Technology & Operations and the Head of Cyber Security. Emergency access accounts must be reviewed quarterly to ensure they remain fit for purpose, withdrawn where no longer required, and must be sufficiently auditable. An emergency access account must be operated solely for the intended purposes and separately from the standard user account.

4.9 **Accounts for non-widely used IT systems/services:** Access to non-widely used IT systems/services will be granted following a written authorisation from the approved authoriser. The following principles must be followed when setting up this type of account:

4.9.1 Access must be unique to the individual (username and password) and not to a group of users (such as a generic account) to establish the identity of the user at all times during the access period.

4.9.2 Access must be relevant and commensurate with the business need. That is, the minimum access that satisfies the business need must be given. For example, where a user requires a “Read Only” view to certain data, the view must only display the required data fields where practically possible, and individuals requiring this access must be given only the “Read Only” view.

4.10 **Delegated mailbox access:** Members of staff may delegate access to their inboxes if they require someone else to access their email, for example, personal

assistants/secretaries, or staff covering a role during periods of temporary absence. Account login details must not be shared with others as an alternative to delegated access.

4.11 **Wireless Visitor access:** Requests for wireless visitor access will only be granted if the requester is affiliated with the university and the request is approved by the relevant authoriser or if wireless visitor access is needed for events hosted by the university.

4.11.1 For events including but not limited to open days, conferences and seminars, event organisers may use Wireless Visitor Access to provide self-service wireless access for guests.

4.11.2 To prevent abuse or misuse of the service, self-service wireless access shall be restricted to the duration of an event, a realistic maximum number of visitors shall be set and unique access details shall be configured for each event. The access details for an event shall be distributed appropriately (e.g. printed on visitor badges, included on a presenters' slide or displayed near a check-in area). The access details should not be publicised on social media, in newsletters or websites or other places where it may be seen by people not entitled to use the service.

4.11.3 Wireless Visitor Access must not be used for generic use. Staff, students and affiliates with dedicated university accounts should use these accounts to connect to the standard wireless service.

4.11.4 Wireless Visitor Access must not be used for commercial activity. This includes, but is not limited to, non-university hosted events such as where university facilities are hired for external events.

4.12 **University Cloud Access:** Standard (staff and students) and Affiliate Account owners will have access to the university's cloud platforms as appropriate for work and study.

4.12.1 Microsoft 365 Teams: Guest access to Teams will be provided by the IT Service Desk when requested by a Team owner. Requests should be made by completing the request form. Users with Guest access can be added to other Teams in 365 and do not require a new request form to be completed for them. Only members of staff are permitted to request guest access to Teams.

4.13 **Staff changing roles:** Line managers or designated staff members must ensure that access to non-widely used IT systems/services and departmental folders are removed for a staff member (this also applies to Jobshop staff) transferring from their departments to other teams or departments within the university. A deactivation request specifying when access should be removed must be sent to the IT Service Desk. Where the same access is required by the staff in a new role, access may not be deactivated. However, the new line manager must review the access to ensure it is commensurate with the access need for the new job role.

5.0 Managing User Accounts

5.1 User accounts are only to remain active for the period required for individual users to fulfil the business or academic need for which they have been granted.

5.2 At the first login to a new user account, the user must change the default password assigned to the account.

5.3 Login details must not be shared with others, and an individual's user account must not be used as a generic account.

5.4 User accounts must not be used to attempt to or gain access to IT resources and information that have not been authorised for these accounts.

5.5 Users must not access other users' accounts. Where it is necessary to allow such access, it must be only for investigatory or IT support purposes.

6.0 Responsibility

6.1 It is the responsibility of all university account owners to adhere to this policy. Line managers are responsible for overseeing adherence to this policy within their respective areas of responsibility.

6.2 University user accounts covered in this policy are only to be created with the appropriate profiles and privileges as defined and authorised by the approved authoriser. It is the responsibility of the system administrator to ensure an account is created following the approved access.

6.3 All individuals who access, use or manage the university's IT systems and information are responsible for reporting any breach of this policy to the appropriate line manager and the IT Service Desk.

7.0 Suspension of User Accounts

7.1 The user account of a staff member will only be suspended on the authority of the faculty operating officer or director. The suspension must be informed by the university's People Directorate investigatory process carried out on the staff member, or where it has been determined that there is a misuse of IT resources or is related to a security incident that could harm these resources or the university's image.

7.2 The suspension of a student's user account will be authorised by the head of faculty or department or by Information and Library Services where it is related to misuse of IT resources or for an investigatory proceeding.

8.0 Policy Compliance

8.1 The necessary steps to verify compliance with this policy shall be undertaken. This includes, but is not limited to, business tool reports, internal and external audits and feedback to the policy owner.

8.2 Failure to adhere to this policy may be addressed under the university's disciplinary processes and relevant contractor and third-party contractual clauses relating to non-conformance with the Information security policies.

9.0 Exception to Policy

9.1 Any exception to this policy must be approved by the Executive Director and Chief Information Officer or a nominee.

10.0 Policy Review and Maintenance

10.1 This policy shall be reviewed annually and where necessary will be updated as part of the continual improvement process.

11.0 Related Policies

- Information Security Policies
- Information Compliance Policies
- Risk Management Policy and Guide