Loughborough University

Information Security

Policy on the Management of User Access to Information

Version 1.4:
Approved May 2022
Review May 2025

www.lboro.ac.uk

Policy on the Management of User Access to Information

1. Policy Overview

Loughborough University implements physical and logical access controls across the: IT Systems, data networks, and information it holds in order to provide authorised, auditable, and appropriate user access; and to ensure appropriate preservation of data confidentiality, integrity and availability.

Access Management systems are in place to protect the interests of both those who have provided information to the University and authorised users of that information.

2. Policy Audience

This policy document applies to:

- Staff in management roles who are responsible for authorising access rights appropriate to individuals in their areas of responsibility.
- Authorised users (new starters, current users);
- Leavers;
- Authorised users moving jobs or changing responsibilities.
- Service providers requesting access to information held by the University, IT Systems or network access;
- Authorised external stakeholders (e.g., research partners).

The majority of this policy applies to user accounts, which are created and managed within IT Services, but the same principles should be applied across the whole University when granting access to information, regardless of its format.

3. Policy Sections

Authorisation of Access

Deans and Heads of Professional Services are responsible for ensuring that there are systems in their School or Service to maintain awareness of the information held and to ensure it is stored, used, and shared only in accordance with university policies and procedures (2(c) of the University Information Governance Policy).

It follows that Schools and Professional Services must have mechanisms through senior staff and line managers for the authorisation of appropriate access to information by members of the School or Professional Service whether that information is held in the School or accessed through university systems and regardless of the format of the information. In relation to access to information held in corporate IT

Systems, the School must have arrangements to ensure authorisation to individuals complies with the access approval procedures for the specific system concerned. These expectations also apply to the management of access to information by service providers and external stakeholders.

Access rights should be authorised following the principles of least privilege and need to know.

Access in Hardcopy Format

Confidential information held in hardcopy format should be kept in locked storage which cannot easily be removed from the room concerned (e.g., locked filing cabinets, safes). Only staff authorised to access the information should have access to the key and they should be provided with specific training to ensure they are aware of their responsibility for maintaining the confidentiality and integrity of the information concerned.

When Confidential information is being used, staff should take care that its content is not visible from ground floor windows and that unauthorised individuals within the building do not have access to it. Rooms should be locked when empty and unauthorised staff should not be left alone in the presence of Confidential information.

Staff are discouraged from taking physical copies of confidential information off-campus. If it is necessary, staff should take care it is located out of sight of unauthorised individuals and when not in use, it is stored in a locked or sealed environment. Additional care must be taken to transport confidential information to and from campus as securely as possible, where upon it shall be returned to locked storage forthwith.

User Accounts

All members of staff, as defined by the University's HR system (iTrent), have an IT account automatically created for them on their appointment and are issued with an initial password (noting exclusions in appendix). If the telephone services are taken the account is assigned telephone number (which may or may not be shared) listed in the telephone directory.

All University students, as defined by the Central Student Record System (LUSI), have an IT account automatically created for them when they complete the on-line student registration process and are issued with an initial password.

The majority of IT systems will utilise this central IT account; therefore, it is important to ensure you keep the password securely and use the account in accordance with the University IT Acceptable Use Policy.

The User Accounts of staff leaving the University will remain active, but not accessible, for 30 days after date of contract expiry which is usually their last working day. Access to some University systems will be removed from the date of contract termination. After 30 days the accounts will be deleted. Further information can be found on the IT User FAQs page.

All student accounts will remain active for 30 days after they have been marked as completing their course in LUSI, which is usually after the date of the programme board (UG and PGT students) or completion of all examination requirements (PGR students) and all tuition fees have been paid. 30 days after then the account will be deleted.

Any additional authorised users at the University who require access to IT Services facilities and services will be provided with an IT account on request and with suitable

authorisation (Deans of Schools, Operations Managers or Heads of Professional Services or delegates) (contact IT.Services Helpdesk for advice.)

Account Types

The different types of accounts which can be requested via IT Services is available in Appendix 1 below.

Tenant accounts

Tenant account holders are tenants of the University and will have IT access on a login only basis if agreed in their contract terms and conditions. Account management between Loughborough University and Tenants falls under the remit of Facilities Management.

Visitor accounts

Visitor accounts are assigned to people who are engaging with the University on a temporary basis and do not fall under the category of Staff or Student. Types of visitor access are staff-like, student-like, login only.

Generic accounts

Generic accounts (many individuals sharing a single username and password) shall not normally be permitted as a means to access Loughborough University data but may be granted under exceptional circumstances if sufficient additional controls on access are in place. Under all circumstances, users of accounts must be identifiable at all times. The business case and control arrangements will be agreed between the relevant School or Professional Service manager and IT Services before the account is created.

Generic accounts will never be used to access information categorized as Confidential or Highly Confidential under the University's Information Categories and Controls Policy.

Third Parties

Third parties (Service providers, contractors and project partners) will be provided with accounts, if necessary, that solely provide access to the systems and / or data relevant to their relationship with the University, in accordance with least privilege and need to know principles. The accounts will be removed at the end of the contract or partnership agreement and will be reviewed at least on an annual basis by the IT Service Desk.

Privileged accounts

The allocation of privileged rights (e.g., local administrator, domain administrators, root access) to information systems shall be managed by IT Services in consultation with School and Service staff with relevant responsibilities. Deans of Schools and Heads of Professional Services must ensure appropriate arrangements are in place for allocation of privileged access rights to any local systems.

Privileged accounts must only be used by systems administrators when undertaking specific tasks which require special privileges. Systems administrators must use their user accounts at all other times.

Keeping Information Secure

Every user should understand the sensitivity of the information to which they have access in accordance with the University's Information Categories and Controls Policy and treat it accordingly. Even if technical security mechanisms fail or are absent, every user should attempt to maintain the security of data based on its information category.

Access to Highly Confidential and Confidential information

Access to Highly Confidential or Confidential information will be limited to authorised persons whose job or study responsibilities require it, as determined by law, contractual agreements, or the Information Governance Policy.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources within Loughborough University's Active Directory infrastructure managed by IT Services.

Management of User Privileges

Management of user privileges should wherever possible be based on group membership or role assignment rather than individual accounts although this will not be appropriate for access to some Highly Confidential information.

A user's access to information systems must be controlled and updated by relevant managers and system administrators when circumstances change. This is to ensure that security risks are minimised and to allow University business to continue without undue hindrance.

- Users' access rights must be adjusted in a timely manner to provide only that access which is authorised and necessary.
- The purpose and membership of all privileged groups and roles should be periodically reviewed by the business owner.
- A periodic general review by the business owner of login accounts should lead to removal of access to those accounts, which are no longer eligible or required.

Compromised accounts and passwords

If a university user account or password is suspected to have been compromised, the incident should be reported immediately to the IT Service Desk, who will follow the appropriate process. Such passwords must be changed as soon as possible. Appropriate arrangements should be made for this eventuality with local systems in Schools and Professional Services.

Misuse of Systems Access

The University can at any time suspend a user's access to a corporate system if it is believed they are sharing account details, conducting malicious or illegal activities.

The Acceptable Use Policy sets out the purposes for which University systems may be used (whether provided by IT Services or locally). Misuse of systems or abuse of access to other University information by staff or students may be treated as a disciplinary offence. Use of systems or University information in relation to criminal activity by staff, students or third parties will be reported to the police.

Appendix 1 - Policy for the Management of User Access

Account Types available from IT Service (excludes access information to specific applications or services)

Identity Type	Account Type	Account Sub-Type	Account Characteristics	Approver	Email	Building Access
Tenant	Login Only		Account holders are tenants of the University and will have IT Access login only if agreed in their T&C's. The relationship is administered by Facilities Management. Printing possible on request, scanning also possible but requires own email address to send on to as LU email will not be provided.	Facilities Management or ITS Business Partnering via Tenant - Raise request straight through to CC	N/A	Optional
Visitor	Staff-Like		Identities that have similar levels of system access to a member of staff, suitable for visiting academic staff or contract and agency staff working in Professional Services	Deans, Ops Manager or Heads of Professional Services	Optional	Optional
Visitor	Student-Like		Has access to learning resources and systems, as if a student, suitable for participants in short courses and other temporary students not registered through LUSI.	Deans, Ops Manager or Heads of Professional Services	Optional	Optional
Visitor	Login Only		Has an Active Directory account but no automatic access to university systems unless manually granted. This category is suitable for example for IT Vendor staff who need to remotely log into a specific system to perform maintenance. This category will also be used to provide library access to members of the public.	Deans, Ops Manager or Heads of Professional Services	N/A	Optional
Visitor	No Access		No IT access is granted.	Deans, Ops Manager or Heads of Professional Services	N/A	Optional
Extended Account (ex-staff or student)	Manually registered		These group of accounts are accounts that were previously provisioned by LUSI or iTrent. They are no longer provisioned by these systems and have had their account extended outside of these system for a reason. The characteristics of these type of accounts is that they are not of employee type 'v' and so may retain the access they had as a student or staff member. They may also retain their previous department access if the department code is not updated to reflect their new position.	Deans, Ops Manager or Heads of Professional Services	By Default	By Default
Staff	Staff	Paid staff	Member of staff as defined by HR, including both paid and unpaid positions. Includes lay members, emeritus professors, external examiners, retired colleagues who continue to teach or support research, and sponsored visiting academics, professors, and fellows.	Human Resources	By Default*	By Default

			*Note, certain postgraduate or claims staff will not automatically have an ITS account created.			
Staff	Staff	Emeritus Professors	Member of staff as defined by HR, including both paid and unpaid positions. Includes lay members, emeritus professors, external examiners, retired colleagues who continue to teach or support research, and sponsored visiting academics, professors, and fellows. *Note, certain postgraduate or claims staff will not automatically have an ITS account created.	Human Resources	By Default*	By Default
Staff	Staff	External Examiners - Taught	Member of staff as defined by HR, including both paid and unpaid positions. Includes lay members, emeritus professors, external examiners, retired colleagues who continue to teach or support research, and sponsored visiting academics, professors, and fellows. *Note, certain postgraduate or claims staff will not automatically have an ITS account created.	Human Resources	By Default*	By Default
Staff	Staff	External Examiners - Research Students	Member of staff as defined by HR, including both paid and unpaid positions. Includes lay members, emeritus professors, external examiners, retired colleagues who continue to teach or support research, and sponsored visiting academics, professors, and fellows. *Note, certain postgraduate or claims staff will not automatically have an ITS account created.	Human Resources	By Default*	By Default
Staff	Staff	Lay Member of Committee	Member of staff as defined by HR, including both paid and unpaid positions. Includes lay members, emeritus professors, external examiners, retired colleagues who continue to teach or support research, and sponsored visiting academics, professors, and fellows. *Note, certain postgraduate or claims staff will not automatically have an ITS account created.	Human Resources	By Default*	By Default
Staff	Staff	Retired/departed staff who still collaborate with research including supervising research students	Member of staff as defined by HR, including both paid and unpaid positions. Includes lay members, emeritus professors, external examiners, retired colleagues who continue to teach or support research, and sponsored visiting academics, professors, and fellows. *Note, certain postgraduate or claims staff will not automatically have an ITS account created.	Human Resources	By Default*	By Default
Staff	Staff	Retired/departed staff who still deliver teaching	Member of staff as defined by HR, including both paid and unpaid positions. Includes lay members, emeritus professors, external examiners, retired colleagues who continue to teach or support research, and sponsored visiting academics, professors, and fellows. *Note, certain postgraduate or claims staff will not automatically have an ITS account created.	Human Resources	By Default*	By Default
Staff	Staff	Visiting Academics (Sponsored)	Member of staff as defined by HR, including both paid and unpaid positions. Includes lay members, emeritus professors, external examiners, retired colleagues who continue to teach or support research, and sponsored visiting academics, professors, and fellows.	Human Resources	By Default*	By Default

			*Note, certain postgraduate or claims staff will not automatically have an ITS account created.			
Staff	Staff	Visiting Professors (Sponsored)	Member of staff as defined by HR, including both paid and unpaid positions. Includes lay members, emeritus professors, external examiners, retired colleagues who continue to teach or support research, and sponsored visiting academics, professors, and fellows. *Note, certain postgraduate or claims staff will not automatically have an ITS account created.	Human Resources	By Default*	By Default
Staff	Staff	Visiting Research Fellows (Sponsored)	Member of staff as defined by HR, including both paid and unpaid positions. Includes lay members, emeritus professors, external examiners, retired colleagues who continue to teach or support research, and sponsored visiting academics, professors, and fellows. *Note, certain postgraduate or claims staff will not automatically have an ITS account created.	Human Resources	By Default*	By Default
Student	Student		Student as defined by Registry	Academic Registry	By Default	By Default
Third Party	-remote		This type of account is provided to external service providers, to allow for remote management of systems or services. This account is created within the directory service provided by IT Services and permissions are granted once a completed remote access document has been received and signed off by the service owner.	IT Services – Service Owner	N/A	N/A
Service Accounts	-svc		This is a service account which is created when a particular service requires access to domain services. This account is created within the directory service provided by IT Services and permissions are granted on the authority of the appropriate service owner.	IT Services – Service Owner	N/A	N/A
Shared Mailbox	@mailbox.lboro.ac.uk		This account provides a shared mailbox with access is controlled by the manager(s) of the mailbox. The account does not expire. Inbound address can have an alias e.g., registry@lboro.ac.uk to support migration (new Shared Mailboxes should not), outbound emails will show as registry@mailbox.lboro.ac.uk	Deans, Ops Manager or Heads of Professional Services	By Default	N/A
Generic Account	Manually Registered		This type of account is only created if there is a valid business case (see below). Includes access requests to filestore. The account is not linked to an individual user but linked to a group of users or a role. An example for this type of role is reception@lboro. The Service Desk within IT Services manually creates this type of account.	IT Services – Senior Leadership Team	By Default	Optional
Visitor	ZZ account		This type of account is primary used for short course or conference attendees who require very short-term access and will be created as a student account. These accounts have fixed expiry dates.	IT Services – Senior Leadership Team	Optional	Optional

Document Control

Version	Author	Date	Version Detail
V0.1	Niraj Kacha	26th Nov 2015	First draft
V0.2	Amendments by Jennifer Nutkins	14 Jan 2016	Revised following IGSC on 11 Jan 2016
V0.3	Niraj Kacha	18th Jan 2016	Updated accounts table and reviewed document
V0.4	Jennifer Nutkins	22 Jan 2016	Minor updates and accepted changes following final comment for submission to Feb ITGC
V0.5	Niraj Kacha	11th Feb 2016	Removed Account type table following recommendation from ITGC
V0.6	Matthew Cook	19th Feb 2016	Added recommendations from IGSC
V0.7	Mark Lister	7 March 2016	To incorporate comments made by ITGC
V0.8	Matthew Cook	9th Mar 2016	Added recommendations from IGSC
V0.9	Jennifer Nutkins	15 March 2016	Very minor amendments following JCN read through.
V1.0	Mike Domokos	23 Sept 2020	Revised to include IDM identity types, BOR and Roadmaps for account types
V1.1	Mike Domokos	5th Oct 2020	Updates with ITS stakeholder feedback
V1.2	Niraj Kacha	1st April 2022	Added clarification around authorisation
V1.3	Niraj Kacha	1st April 2022	Updated account types table
V1.4	Claire Vallance	11 April 2022	Added instructions for using physical information formats off-campus

Review/Approval History

Organisation	Action	Date
IGSC	Approved	8/10/20
ITGC		27/10/20
IGSC	Approved	05/05/2022
ITGC		26/05/2022