LSE Governance

Policy

IT User Accounts

Jethro Perkins

Information Security Manager

Summary	This document defines the policy around the issuing and revocation of user accounts of all types. It includes conventions for user IDs for students, staff, generic accounts and service accounts.
Version	3.9
Date	16 October 2015
Library reference	ISM-PY-016

Document control

Distribution list

Name	Title	Department
Puneet Singh	Systems Manager	Infrastructure, IMT
Jethro Perkins	Information Security Manager	IMT
Mike Bragg	Systems Specialist	Infrastructure, IMT
Nic Warner	STICERD IT Manager	STICERD
Information Security Advisory Board		
Information Technology Committee		

External document references

Title	Version	Date	Author
Information Security Policy	3.0	15/03/2013	Jethro Perkins
Conditions of Use of IT Facilities at LSE	2.2	13/03/2013	Jethro Perkins
Jisc Acceptable Use Policy (https://community.jisc.ac.uk/library/acceptable-use-policy)	11	May 2011	S.Wood

Version history

Date	Version	Comments
12/06/13	3.0	Rewrite by Information Security Manager of old version.
14/06/13	3.1	Update of processes, inclusion of initial work with HR,
17/06/13	3.2	Brought in line with new Information Security Policy, Access Control Policy
19/06/13	3.3	Incorporated comments from Mike Bragg
01/07/13	3.4	Further queries from Mike Bragg about Short Course students not being held in SITS addressed
06/08/13	3.5	Incorporation of issue of requests for early termination of accounts from staff and students
31/10/13	3.6	Incorporated reference in 3.1.9 to Procedure ISM-PD-104 'Assigning Administrative Accounts on local machines'
20/11/13	3.7	Incorporated external user accounts for research collaboration
19/03/14	3.8	Alteration to reflect ITC queries. 'Summer School' account (Section 3.3.4) expiries amended to end of August, and LSE SU executive staff explicitly included under 'staff' (Section 3.3.12)
16/10/15	3.9	Altered section 3.1.2 to clarify when the use of generic accounts could happen, and where they are not permitted.

Review control

Reviewer	Section	Comments	Actions agreed
ITC	3.3.4	Why do Summer School Students seem to have a longer expiry than standard students?	This was a misunderstanding based on the difference between account expiry and account deletion. This has been rectified in v 3.8.

ITC		No reference in the document to LSE SU staff	LSE SU staff are treated for account purposes as staff. This has been explicitly included in Section 3.3.12
HSCIC	3.1.2	The title of 3.1.2 implies that accounts could be issued to more than one person. This is absolutely not permitted under any agreement to access HSCIC data.	Section 3.1.2.1 has been added to clarify the situation. There are shared accounts in use at LSE, but they would in no way be used for access to any personal or research data (including HSCIC data)

Table of contents

1 Introduction

1.1 Purpose

There is a requirement within the LSE to define the policy around the creation, deletion and use of **IT User Accounts** within the LSE. This document sets out the agreed types of account that may be used and the responsibilities that come with being allocated one.

1.2 Scope

This document relates to all IT User Accounts created within the LSE for authorisation to LSE IT resources, including access to LSE-provided Internet services. It covers both internal and external users, either studying or working at LSE, or those who wish to register for access to Internet-based resources.

This document covers the conventions for user IDs. It does not cover conventions regarding the assignation of e-mail addresses and aliases; these are covered in a separate document.

1.3 Background

There is a requirement within the LSE to have a policy covering IT User Accounts to enable the School to provide access to those individuals and organisations that it wishes to in order to further the aims of the School. It will make the creation and allocation of login credentials more consistent and also allow the School to be confident that obligations for various services that the LSE subscribes to are being met. It will also allow conformance with the Information Security Audit recommendations[i].

There are also legal obligations on the LSE, such as Data Protection, that are reliant on a certain level of confidence in the usage of user accounts.

In addition, use of the LSE's connection to the Joint Academic Network and the Internet is governed by JANET's Acceptable Use Policy, which states that:

> *"9. Subject to clauses 11 to 19 below, JANET may be used by a User Organisation and its Members for any lawful activity that is in furtherance of the aims and policies of the User Organisation.*
>
> *...*
>
> *22. A User Organisation may extend JANET access to other individuals on a limited basis where this is done in pursuance of the User Organisation's remit and for which it receives public funds, provided no charge is made for such access.*
>
> *23. It is expected that such use will be regulated by the User Organisation in the same manner as it would regulate occasional use by third parties of its other facilities, such as its telephone and IT support systems. Any individual using JANET in this manner must therefore be subject to the same requirement to use JANET in an acceptable manner as is required by the User Organisation of its Members."*

1.4 Assumptions

Departments creating records in LSE Central[ii] are responsible for verifying individual users' identity.

Legacy accounts may not conform to this policy.

LSE wishes to create accounts for a number of different types of user in different systems.

[i] Internal Audit Report: Information Security, BDO, April 2011, as submitted to Audit Committee as paper AuC/11 on 1 November 2011.

[ii] LSE Central is the database which provides a unique identifier to each user object contained within it.

The categories of user described in this policy are not rigid; some people may assume roles that incorporate elements of different categories. Not every combination of role is described in this document.

1.5 Conventions

A number of different styles of text and page layout are used within this document. This section describes the use of these styles together with examples.

1.5.1 Font styles

Bold is used to emphasise important information.

Italic is used for file and directory names, URLs and registry key names. Italic is also used to indicate a filename or comments within a code section. Italic is also used for the first reference to a vendor or product where doing so improves clarity.

1.5.2 Bullets

Bullets appear indented in relation to the paragraph indentation with a nested bullet available in a different style:

- Bullet
    - Nested bullet

1.5.3 Tables

Tables appear as follows:

Header Row (Repeated on each page if the table splits across a page)
Data Row

2 Responsibilities

2.1 User responsibilities

All people using IT User Accounts to access LSE systems must adhere to the *Conditions of Use of IT Facilities at LSE*. These can be found at:

http://www2.lse.ac.uk/intranet/LSEServices/policies/pdfs/school/conOfUseOfITFacAtLSE.pdf

Individual systems may have additional conditions.

2.2 Account creation staff (in IMT and elsewhere)

All staff creating IT User Accounts must adhere to the contents of this policy. Queries or suggestions should be made to the School's Information Security Manager.

Where the creation of an IT User Account involves creating a new LSE Central record, checks must be made to verify the identity of the individual before providing access to the account.

2.3 Account authorisation

Where staff or processes are providing authorisation to resources for IT User Accounts, appropriate checks must be made to ensure that access is granted only with the permission of the resource-owner.

Access to systems and resources outside the default staff provision of email and H: space is provided on a case-by-case basis by the resource owners (e.g. SITS in ARD, Resourcelink in HR, departmental shared folders by Departmental Managers).

The authorisation and auditing processes involved in granting access to these resources is the responsibility of the system owners.

2.4 Directories

LSE currently has no single authoritative directory. ISM-SD-010: "Description of Directories" provides technical staff with an overview of where different IT User Accounts are stored and the criteria by which they can be populated. Those criteria and the criteria contained within that document should be consistent. Where there is a clash, this document takes precedence.

2.5 Exceptions

The Information Security Manager has day-to-day responsibility for managing this policy.

Any disagreements will follow the IMT *Common Exceptions Process* (see ITS-PC-002 CommonExceptionsProcess). For more information, please contact the Information Security Manager.

Any exceptions must be carefully considered, as the possession of an IT User Account can provide wide-ranging access to the network, possibly breaching agreements the School has for effective account management.

2.6 Ownership

This policy is owned by the Director Information Management and Technology.

2.7 Authority

This policy will be reviewed and amended by the Information Security Advisory Board and sent for endorsement to the Information Technology Committee

3 Policy

3.1 Basic Principles

3.1.1 Every user shall have one identity within the LSE.

The User ID that is given shall be consistent with all systems across the LSE. There should not be a need to have multiple, different user IDs, save for in exceptional circumstances where elevated permissions are required (see 3.1.8 and 3.1.9). This does not necessarily imply password synchronisation between systems.

The reason for this is to ensure that all IT User Accounts can be reconciled with an individual user and can be de-provisioned effectively when the user is no longer at LSE.

3.1.2 Every user account shall be used only by the person or persons it was issued to.

It is vitally important that only the person who should be using the IT User Account, actually is. If this is not strictly adhered to, the ability to audit individual actions is diminished.

If an IT User Account is misused, the person to whom the account was issued must take sole responsibility for those actions, regardless of who was actually using the IT User Account at the time.

The reason for this is that in order to audit incidents there must be confidence that the user account is used by the person it was assigned to. The IT User Account is the only way to identify a person from an action and trust must be maintained that the relationship between the person and the account is unique.

3.1.2.1 Shared accounts will only be issued in exceptional circumstances

There may be some exceptional circumstances that require the issuing of accounts for shared use e.g. some classes involving external users or classrooms utilizing test conditions. These must be explicitly authorised by the Information Security Manager. However:

- *All* shared accounts must still maintain personally-identifiable use, as mandated by our Internet Service Provider, Jisc, under their Acceptable Use Policy (https://community.jisc.ac.uk/library/acceptable-use-policy) for access to the Janet network
- All shared accounts will have an accountable person, who will agree to take responsibility for all behaviour conducted using the account
- No generic account or shared account will be permitted access to any systems or storage containing personal data or research data. Only accounts explicitly linked to defined individuals will be provided access to such data, and then under least privilege and need to know principles, or as otherwise defined in and governed by third party contracts or data sharing agreements.

3.1.3 User IDs or email addresses shall not, after account retirement, be re-used for a minimum of 24 months.

A system is in place to ensure that user IDs and email addresses shall not be re-issued within 24 months of the account's disablement or deletion, in accordance with the user account lifecycle process. Nor shall they be assigned to "non-person" entities, such as departmental mailing lists.

There are two main reasons for this. Firstly, it is a requirement for LSE's membership of the UK Access Federation[iii]. Secondly, experience has shown that re-using an account too

[iii] The UK Access Federation provides a single solution for its members to access online resources and services for education and research. Its use is governed by Rules and a legally-binding agreement. Details here: http://www.ukfederation.org.uk/content/Documents/Documentation

quickly means that the new owner receives lots of newsletters and messages intended for the previous owner: a two-year window allows the senders to remove disabled mail accounts through their receipt of non-deliverable message reports.

System owners of services that rely on Active Directory accounts but replicate user IDs locally for authorisation purposes must check for instances where user IDs are deleted or re-issued. It is their responsibility to remove expired accounts from their systems.

'ITS Reg' provides user deletion logs held in Oracle that can be used for checks.

3.1.4 Individual IT User Accounts for use with core LSE systems can be created only if the owner has an associated record in LSE Central, or is linked to an existing account

For data integrity purposes, internal IT User Accounts can be created only if the user in question has an entry in LSE Central or another user takes responsibility for creating their account. .

The reason for this is to ensure that every IT User Account is associated with a responsible person at LSE and sanctions can be levied against them in the event of misuse of the account.

Where users are accessing resources that have no impact on those provided by IMT (in STICERD, for example), this prerequisite does not apply. However, such IT User Accounts may have limited or no access to other LSE systems.

3.1.5 All user accounts must reside in systems authorised by IMT[iv]

Directories must only be created in conjunction with IMT. New applications that use existing directories for authentication purposes must be discussed and agreed with IMT via approval of an ITPB project proposal prior to implementation.

The reason for this is to prevent a proliferation of user directories, which would result in increased maintenance costs and increase the risk of disparate identities for a single user. In addition, those directories authorised by IMT will have a security configuration not guaranteed by unknown directories.

3.1.6 All accounts must adhere to the principle of least privilege

The level of access to resources granted to an IT User Account should be commensurate with the privileges required by the owner to do his or her job, and no more.

This is so that accidental damage is limited, for example if a standard user is added to the local administrative group, a virus downloaded will spread with the same rights. In a database or application context, limiting access removes the temptation to access information that someone should not have access to, which also protects LSE from breaking the Data Protection Act.

3.1.7 All users with access rights to LSE resources and facilities must agree to the *Conditions of Use of IT Facilities at LSE*

This document outlines the responsibilities that users have when accessing LSE resources. This is so that everyone is aware of their rights and responsibilities.

It is not required for limited-access IT User Accounts, where no internal resources are used.

Breaches of the 'Conditions of Use' (for example, by the accidental or deliberate disclosure by an individual of their username and password details) will lead to a requirement to re-read and re-sign the policy, and in severe or repeated cases will lead to further actions as documented

[iv] The term "IMT" in this context encompasses IMT, the Library's IT team, the Centre for Learning Technologies (CLT) and RLAB (STICERD and CEP).

in the 'Conditions of Use', 'Information Security Policy', 'Data Protection Policy' or as deemed appropriate by HR.

3.1.8 IT User Accounts with administrative privileges used remotely

As mandated in the Remote Access Policy, any remote use of administrative functions should be protected by two factor authentication.

This is to limit the risk of outsiders being able to "hack" accounts that could do serious damage across the whole of LSE rather than limited to the scope of a "standard" user account and to minimise the level of damage that could result from a user accidentally leaving such a device unattended and still logged in.

This provision is not yet in place.

3.1.9 Administrative IT User Accounts should not be used for day-to-day activities

Where users with privileged IT User Accounts (i.e. those with elevated access permissions) need to access the Internet or read e-mail, this should be done using an account without administrative privileges.

The reason for this is that any malicious software inadvertently downloaded while using a privileged account will spread across the domain using the same privileges as the account used to download it.

The assignment of accounts with Administrative privileges will be audited, and an appropriate account (with formal 'admin_xxx where xxx is the standard LSE username of the user requesting admin access) will be created.

The process for recording the assignment of admin accounts is laid out in Procedure ISM-PD-104 'Assigning Administrative Accounts on local machines.'

3.1.10 All User IDs shall be assigned by IMT or authorised LSE Staff

All User IDs to identify individuals shall be assigned by IMT or staff authorised by IMT where there is an operational need.

3.2 Access levels

There are a number of different levels of access that can be granted to individual users, depending on their type. The table below describes these levels.

Access level	Description
1	Access to specific externally available applications
2	Authenticated Internet access only from LSE
3	Active Directory account for logging on to LSE domain, but only to specific applications and logged access to the Internet
4	Full Active Directory account and email - lower initial quota
5	Full Active Directory account and email - higher initial quota

3.3 Different types of accounts

Different types of user are entitled to different levels of access, depending on their relationship with LSE and what the primary purpose for being at LSE is. More clarification on the compliance elements of this can be found in the JANET Acceptable Use Policy[v].

[v] http://www.ja.net/company/policies/janet-aup.html

3.3.1 Undergraduate student

3.3.1.1 Description

This is a student registered to do an undergraduate course and registered through and active within the student record system, SITS. Terminates when completed, suspended or withdrawn.

3.3.1.2 Access Level

Access level 4.

3.3.2 Postgraduate student – taught

3.3.2.1 Description

This is a student registered to do a postgraduate taught course and registered through and active within the student record system, SITS. Terminates when completed, suspended or withdrawn.

3.3.2.2 Access Level

Access level 4.

3.3.3 Postgraduate student – research

3.3.3.1 Description

This is a student registered as doing research and registered through and active within the student record system, SITS. Terminates at the end of the year study is marked as completed in SITS, study is suspended or the student withdraws.

3.3.3.2 Access Level

Access level 5.

3.3.4 Summer School student

3.3.4.1 Description

A student who has paid to do a course through LSE's Summer School. Terminates when completed, suspended or withdrawn. Registered in SITS – record of start and termination dates feed into account expiry settings. Summer School accounts expire at the end of August, unless the account is linked to further study or other engagement with LSE.

3.3.4.2 Access Level

Access level 4.

3.3.5 LSE Enterprise student

3.3.5.1 Description

Delegates on courses run by ELSE. Terminated when completed, suspended or withdrawn. Account allocation and de-allocation dates registered in database – fed into account expiry settings.

3.3.5.2 Access Level

Access level 4.

3.3.6 TRIUM student

3.3.6.1 Description

Students registered to do a TRIUM course and registered within and active in the student record system, SITS. Terminates when completed, suspended or withdrawn. Account allocation and de-allocation dates registered in database – fed into account expiry settings.

3.3.6.2 Access Level

Access level 4.

3.3.7 Short course student – Full time

3.3.7.1 Description

Students registered on a short course, registered and active within a short course database. Terminates when completed, suspended or withdrawn. Account allocation and de-allocation dates registered in database – fed into account expiry settings.

3.3.7.2 Access Level

Access level 4.

3.3.8 Short course student – flexible learning with Moodle

3.3.8.1 Description

Students registered on a short course, registered and active within SITS but who require only access to Moodle and will not be full-time at LSE. Terminates when completed, suspended or withdrawn. Account allocation and de-allocation dates registered in database – fed into account expiry settings.

3.3.8.2 Access Level

Access level 1 – Moodle and electronic Library resources

3.3.9 Short course student – other

3.3.9.1 Description

Students registered on a short course, registered and active within SITS but who have no requirement for access to any LSE resources.

3.3.9.2 Access Level

None.

3.3.10 Alumni

3.3.10.1 Description

An alumnus/a is a former student of the LSE who has completed at least one continuous term of a course of study. This does not include External Degree holders, Summer School, Language Course, Occasional students etc. who do not register as students at the School

3.3.10.2 Access Level

Access level 1 – Houghton Street Online. There is no time limitation on Alumni accounts.

3.3.11 Friends and family of student

3.3.11.1 Description

Nominated (but limited) friends and family are granted limited access to externally accessible resources to allow updates to next of kin information.

3.3.11.2 Access Level

Access level 1 – LSE For You.

3.3.12 Staff: salaried or hourly paid, and with a contract of employment

3.3.12.1 Description

Members of staff who are paid via Payroll and have a contract of employment with LSE, including full time members of staff, part time members of staff, hourly-paid staff, students employed as staff, research assistants and graduate teaching assistants, User accounts are withdrawn at the termination of contract where this does not conflict with the completed student grace period of one term- end of year.

Members of LSE Students' Union executive are issued accounts that are treated as staff in this category. Accounts are withdrawn or extended upon information from the SU executive.

3.3.12.2 Access Level

Access level 5.

3.3.13 Staff – contract or temporary

3.3.13.1 Description

Members of staff who are paid via a third party who invoices LSE, including contract staff, agency staff and consultants. An account is provided on request from the department admin or line manager who should also request deletion when the contract ceases.

3.3.13.2 Access level

Access level 5.

3.3.14 Former members of staff

3.3.14.1 Description

Former academic members (e.g. Emeritus academics) and administrative members of the School, where the relevant Head of Service/Department has explicitly agreed to it.

3.3.14.2 Access level

Access level 5.

3.3.15 LSE Enterprise staff – administrative staff

3.3.15.1 Description

Staff of LSE Enterprise who work full-time for LSE Enterprise. LSE Enterprise staff have HR records and the account will expire when the HR record is closed.

3.3.15.2 Access Level

Access level 5.

3.3.16 Academic Visitors

3.3.16.1 Description

Academic Visitors, who are registered with HR, are treated as members of staff and have the same level of access.

Academic Visitors *not* registered with HR will have dates for joining and leaving outlined to IMT by Departmental Managers in an ad-hoc manner.

Access Level 5.

(Note: visitors from many other academic institutions may be able to access the Internet wirelessly using the Eduroam service)

3.3.17 Guests and visitors of the LSE attending an LSE-arranged event or on other School-business

3.3.17.1 Description

Visitors or guests who are primarily at LSE in relation to the School's mission, i.e. teaching, research, engagement, access can be granted and terminated when they leave.

3.3.17.2 Access Level

Access level 5, ***except* speakers, delegates and the Press at LSE conferences and events where Access level 2 – *Internet Only* shall apply.**

3.3.18 Other Visitors and Guests including those whose association with LSE is purely commercial in nature

3.3.18.1 Description

Speakers, delegates and press at non-LSE organised conferences and events, commercial guests in LSE halls of residence, commercial users/tenants of LSE space, visitors to the Library and other public access areas, visitors to LSE catering outlets.

3.3.18.2 Access Level

Access level 2 – Internet only

3.3.19 Governors

3.3.19.1 Description

Members of the LSE's Court of Governors and Council.

3.3.19.2 Access Level

Access level 5.

3.3.20 Suppliers

3.3.20.1 Description

Representatives of third party firms setting up or administering LSE on-site systems.

3.3.20.2 Access Level

Access Level 3. Access is only given via individually-named AD accounts to the specific applications required for maintenance / installation, at the minimum permission levels possible to carry out the task involved, for the minimum time the task requires. The accounts with otherwise be deprecated from any elevated privilege groups and disabled.

3.3.21 Generic accounts

Generic or group IDs shall not normally be permitted as means of access to LSE data, but may be granted under exceptional circumstances if sufficient other controls on access are in place.

3.3.22 Service Accounts

Service Accounts are those provided to systems to effect log-on without human intervention (e.g. to access a database), or those given to external software or system maintainers in order to support systems. These:

- Must not have interactive logon rights;
- Must have an explicitly identified owner, who has confirmed acceptance of the *Conditions of Use of IT Facilities*.;
- Should expire after a year, when the owner's account expires or set to expire at the end of the projected life of the service.

Service Account holders can only be issued in accordance with the *Service Account Supplementary Policy*, which is appended as **Appendix D** to this document.

3.3.23 External or Public Accounts

These are IT User Accounts allocated to users outside the School for certain limited functions. External or Public users include but are not limited to prospective students, parents/guardians of students, friends and supporters of the LSE, suppliers, visitors to the LSE website or LSE For You. These:

- Must expire annually (or sooner);
- Must not have an Active Directory domain logon.

3.3.24 External accounts for research collaboration

These are LSE Active Directory accounts used by external parties for collaboration with LSE research projects and use of LSE IT resources in order to facilitate collaborative working. These:

- Must have no email account
- Must be named explicitly in accordance with LSE conventions, with the addition of an EXT prefix
- Must provide access only to the resources required, following the principal of least privilege
- Must have an expiry date agreed in advance
- Have an explicit LSE owner, who will take full responsibility for the actions performed by the users of the account
- Be recorded in an external user security group

3.4 Expiry, Deletions and Suspensions

3.4.1 General Principles

A simple determination of the number of days an IT User Account has been inactive is not a reliable metric to determine a user's status within the School.

An IT User Account should only exist for as long as strictly necessary to prevent its use by someone that LSE cannot sanction for misuse. It is desirable, therefore, to disable an IT User Account as quickly as practicable.

All IT User Accounts will expire annually. Where there is an integrated system that holds details of a particular user that can confirm that this user still has a relationship with the School, their account will, under normal circumstances, be renewed automatically.

System owners of services that rely on Active Directory accounts but replicate user IDs locally for authorisation purposes will need to create checking routines to ensure they are aware when user IDs are deleted or re-issued.

User accounts marked as 'staff' but which have NO open HR record will expire after 6 months unless there is Departmental Manager intervention.

Staff or students requesting early termination of their user accounts (before the end of the employment contract or study period) will have their account disabled until the point of contract / study expiry, when the account will be deleted.

3.4.2 Specific examples

3.4.2.1 Students

Student IT User Accounts will expire three months after the date of graduation or at the end of December in the year of graduation. Until this time, they will still hold the status of student.

Where students are on short courses, the user account will be disabled at the end of the month during which the course terminates.

3.4.2.2 Staff

Where staff details exist in the HR system, their IT User Account(s) will renew automatically, as per above. In the case of contract staff, the Departmental / Divisional Manager responsible for the staff member will be asked to confirm the status of the account.

By default staff accounts will expire upon termination of contract, unless a request for an extension is received from the relevant Departmental Manager.

Line managers will be able to gain access to the mailboxes and data of departed staff up to 1 month after a member of staff has left and the account has been disabled, subject to a written request to the Information Security Manager.

3.4.2.3 Emeritus Professors, Governors and other user accounts

Where an IT User Account is independent of the HR or ARD processes, e.g. Emeritus Professors, the account must be approved by a Departmental Manager who will be asked, each year, to confirm that the account in question should be renewed. Once confirmed, the account will be renewed manually. Where possible, Human Resources will maintain a list of Emeritus academics that should have IT User Accounts and the system would either renew these accounts in the same way as staff or the accounts would be renewed manually.

Emeritus staff will be asked once per year to contact their Departmental Manager in order to renew their LSE IT account.

Accounts of Governors will be kept open until IMT is informed by the Governance Officer, PCPD that an individual is no longer a Governor.

Other accounts will expire annually and will be re-enabled under request from Departmental and / or Divisional Managers.

3.4.3 Suspensions

Under certain circumstances (e.g. in the event of an HR-sanctioned investigation, suspected misuse of the IT User Account, or if the user it was assigned to has left LSE) an IT User Account may be suspended. A number of people may suspend an account. For more information, please refer to the Information Security Manager.

3.4.4 Deletions

Periodically, disabled and expired IT User Accounts will be deleted, along with their associated data. Once an IT User Account has been disabled through the normal process of expiry, there should be no expectation of retrieval of the associated data. Departments and Services should actively consider retaining LSE data that may be of value *before* a person leaves. A checklist of issues to consider as part of the leaving process of any staff member is provided at http://www2.lse.ac.uk/intranet/LSEServices/IMT/about/policies/documents/leaversChecklist.docx

3.5 Conversion of Types of IT User Accounts

It is possible to convert staff accounts to student, and vice versa.

3.6 Conventions

All User IDs shall follow the conventions laid out in this document, including those in systems not managed by IT Services.

3.6.1 Staff, student and guest accounts

All user ids shall take the form:

Surname + two, one or three initials + identifier (if required).

Therefore, if there are several J A Smiths, one of their user IDs will be.

However, if a name is unique, it is acceptable to drop the identifier.

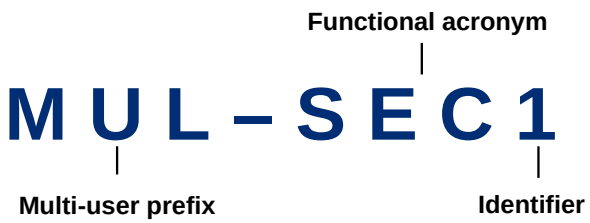
The limit on the number of characters in a User ID is currently eight characters.

3.6.2 Generic accounts

3.6.2.1 Multi-user accounts

Wherever possible, all new IT User Accounts where more than one person is authorised to log in must use a descriptive, functional name, preceded with “MUL-“. This helps to identify multi-user accounts in Active Directory and will allow them to be programmatically ignored in the event that dormant account removal is done automatically.

Therefore, a multi user account for Security might be:



3.6.2.2 Non-User Specific accounts

All accounts must have an explicitly identified owner, who is responsible for the management of the account. Any accounts for which the owner cannot be identified may be disabled at the discretion of IMT.

3.6.3 Service accounts

All new Service Accounts shall have the prefix “svc”, followed by a descriptive name of the service the account relates to. The Exchange service account would be:

3.7 Exceptions

It is acknowledged that legacy IT User Accounts will not conform to this policy and it is operationally problematic to rename some accounts where they already exist. However, all newly created IT User Accounts should conform to this policy.

All exceptions will be handled using the IT Services *Common Exceptions Process* (see document ITS-PC-002 CommonExceptionsProcess) as described in Section 2.5 of this document.

Appendix A Account Schedule

Account Type	Lead time	Expiry
Undergraduate student	None	Renewed every 12 months
Postgraduate student – taught	None	Renewed every 12 months
Postgraduate student – research	5 days, if not automatic	Renewed every 12 months
Summer School student	Within 10 days of enrolment data receipt	End of August
ELSE student	Within 10 days of enrolment data receipt	6 months
TRIUM student	Within 10 days of enrolment data receipt	6 months
Short course student – Full time	Within 10 days of enrolment data receipt	Duration of course
Short course student – flexible learning with Moodle	Within 10 days of enrolment data receipt	Duration of course
Short course student – other	5 days, if not automatic	Duration of course
Alumni	None	Life
Friends and family of student	n/a	n/a
Staff – permanent	2-5 days	Renewed every 12 months
Staff – temporary	2-5 days	Renewed every 12 months
Former members of staff – Emeritus Academics	Manually	Renewed every 12 months
ELSE staff – administrative staff	2-5 days	Renewed every 12 months
ELSE staff – not otherwise employed by LSE	2-5 days	Renewed every 12 months
Guests and visitors	5 days	Length of visit
Conference / Hotel guests	n/a	Length of visit
Generic accounts	2-5 days	Renewed every 12 months
Temporary, individual accounts (Non-user specific accounts)	2-5 days	Renewed every 12 months

Permanent, group account (multi-user accounts)	2-5 days	Renewed every 12 months
Service Accounts	2-5 days	12 months, owner's account expiry or end of projected system life
External Accounts	None	n/a

Appendix B Glossary

Term	Definition
IT User Account	A particular instance of a User ID associated with a person.
Administrative privileges	Where the rights of an account have the potential to affect the authorisations of another user's account or gain access to their data.
JANET	The Internet provider for all UK HE institutions
LSE Central	The system that holds the unique ID for each instance of a user.
Play_ref	A unique identifier in LSE Central for an instance of a person.
Service Account	An account associated with a computer process, not a user.
User ID	An identifier for an individual that may be reused for someone else.

4 Appendix D Service Accounts

Service Account Supplementary Policy: the process for allocating, monitoring and revoking IT User Accounts for Service Accounts, Suppliers, Systems Maintainers and other third parties.

THIS POLICY FORMS Appendix D of the IT USER ACCOUNTS POLICY (ISM-PY-016)

1. Purpose of this Supplementary Policy

From time to time, suppliers and others require IT User Accounts for specific systems to effect log in without human intervention (e.g. to access a database) or for maintenance purposes (e.g. a systems maintainer in order to support systems). These accounts may have elevated permissions and need careful management to ensure that

a) They are only granted when absolutely necessary;
b) Third parties understand their obligations;
c) Each IT User Account is sponsored by an **LSE Owner ("the Sponsor")**;
d) They are routinely monitored;
e) Risk of third party access to LSE systems is minimised.

2. Policy Statement

The *IT User Accounts Policy* (ref. ISM-PY-016) clearly sets out the criteria for allocating a **Service Account** (section 3.3.22), namely such accounts:

- Must not have interactive logon rights;
- Must have an explicit identified owner;
- Should expire after a year, when the owner's account expires or be set to expire at the end of the projected life of the service.

Service Accounts can be allocated for the following purposes:

- For an LSE system to automatically (and without human intervention) log in to another LSE system, e.g. for the purpose of reading from or writing to a database, or to send or receive email, or to write or read other data);
- For an LSE system to automatically (and without human intervention) log in to third party system, e.g. for the purpose of reading from or writing to a database, or to send or receive email, or to write or read other data);

Service Accounts should, in addition to the criteria set out above, be:

- Allocated for the minimum time necessary;
- Conform to the naming convention set out in 3.6.3 of the IT User Accounts Policy (i.e. User IDs will have a "svc" prefix to identify the fact that it is a service account
- All Service Accounts will adhere to the *IT Passwords Standard* (ISM-SD-009) and *Password Change Policy* (itsweb.lse.ac.uk/Teams_and_Groups/Teams/Systems_Team/Information%2C_Policies_and_Processes/Policies/Password_Change_Policy);
- Used only for the purpose for which they were granted.

All third parties and LSE Service Account Owners will be required to sign a document confirming:

- their understanding and acceptance of this policy;
- that the account will not be used for any illegal purposes or for those which may bring the School into disrepute;
- compliance with the *Conditions of Use of IT Facilities at LSE* (www2.lse.ac.uk/intranet/LSEServices/policies/pdfs/school/conOfUseOfITFacAtLSE.

pdf), *the Information Security Policy* (and any supporting policies) and the *JANET Acceptable Use Policy* (www.ja.net/documents/publications/policy/aup.pdf);

- an understanding that a Service Account may be disabled at any time and without prior notification if LSE suspects misuse or if it suspects that an account has been or may become compromised; and
- that data created, used or transmitted by any Service Account may be intercepted for the purpose of investigation into breach of the Conditions of Use of IT Facilities at LSE or for other compliance reasons.

3. Process for the allocation of Service Accounts

a) The Third Party (**"the Requester"**) or the LSE Owner (**"the Sponsor"**) submits a **Request for a Service Account ("the Request")**. This must include:
   - Details of person requesting;
   - Details of person(s) requiring access (if different);
   - Access requirements (systems, permissions);
   - Period of access required (not more than 12 months. Longer periods by renewal of this process);
   - Likely usage patterns (noting that deviation from these might trigger investigation for suspicious activity).

b) The **Request** is sent to the Account **Sponsor** (the person who accepts ownership of the IT User Account). This would normally be in the department/service sponsoring the account or in IT Services for a system-level account).

c) The original **Request** plus the **Sponsor's Approval** then goes to the relevant IT support team

d) The IT support team creates the necessary documentation: **IT User Account Form** with *Conditions of Use* appended; a Statement of any limits of access; A form showing acceptance of the *Conditions of Use*, the *Information Security Policy* (and any supporting statements), the *IT User Account Policy*, and *JANET's Acceptable Use Policy*.

e) Documentation then to be signed off by:
   - The **Requester**
   - The **Sponsor**
   - The **School's Information Security**.

f) The documentation and email chain is logged and captured in SupportWorks – scanned copies of signed documents are acceptable.

g) The relevant IT support team (or the relevant ITS team for the case of system-level accounts) then updates the **Third party Account Log** (spreadsheet, located here: \\deptshared\i\ITS\Shared\Service-Management\Service Accounts).

h) A calendar reminder is diarised to check the account usage after the first 3 months, 6 months and then one month before account expiry, so that appropriate reminders can be sent out for this process to renew.

i) IT User Accounts will be suspended: on expiry, on suspected breach of the Conditions, if the usage pattern varies considerably from what was stated, and/or if any part of this process is not followed.