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.