# London School of Economics & Political Science

## IMT

# Policy

## IT Asset Management

**Jethro Perkins**
**Information Security Manager**

| | |
|---|---|
| **Version** | 1.0 |
| **Date** | 14/03/17 |
| **Library reference** | ISM-PY-150 |

# 1 Introduction

LSE has a responsibility to manage its both its IT *and* Information Assets, which stems from a number of requirements:

- Legal / Regulatory
  - General Data Protection Regulation (personal data / information asset management / data breach management)
  - Data Protection Act
  - Computer Misuse Act
- Contractual
  - Security requirements (e.g. encrypted hard drives, OS and software updates)
  - Equipment lifecycle management (commissioning and disposal)
- Licensing
  - Appropriate products on appropriate machines, as per corporate or individual licensing stipulations

## 1.1 Purpose

This policy aims to ensure that all LSE-issued IT devices report appropriate information to centralised information stores, in order for LSE to provide better assurance it is meeting its legal, regulatory, contractual and licensing requirements.

Under the General Data Protection Regulation, individual contracts with data suppliers, and LSE's duty of care to its community, it is important to ensure that information on IT assets is protected, maintaining the principles of 'least privilege' and 'need to know'.

## 1.2 Scope

All IT devices purchased, run, managed or issued by LSE.

## 1.3 Out of Scope

Personally owned IT devices, or devices issued by other organisations. Users of such devices should, however, be aware of and abide by their obligations under all applicable laws, the LSE's *Information Security Policy*, *Conditions of Use of IT Facilities at LSE*, subsidiary policies, any research contracts and all licensing agreements when these devices are used to access, store or process data where LSE is either the data controller or the data processor.

Local printers and other 'dumb' devices onto which agents cannot be installed must be recorded via asset tags. All devices purchased via IMT will have such asset tags; it is the responsibility of other purchasers to ensure such items are appropriately recorded.

# 2 Policy

## 2.1 IT Device Asset Management

All IT devices purchased, run, managed or issued by LSE will report to centralised, IMT-run asset management stores, or otherwise be manually added to such a store if automatic reporting is not possible. Given the diverse nature of IT equipment (from network switches to phones) there will be more than one centralised asset management store.

In RLAB, where IT administration is fully devolved to a departmental IT function, that IT function can either use the central registers or maintain its own IT asset management store and make it available upon request.

*Information* asset management will be covered by a separate policy, in accordance with the requirements of the EU General Data Protection Regulation.

## 2.2 Asset Management clients

By default, IT Devices will communicate with centralised asset management stores using IMT-provided clients.

Users with admin rights must not remove IT Asset Management clients, or in the event they are provided with an unconfigured asset, must ensure the appropriate asset management client is installed.

## 2.3 Software

Any software installed must be legitimately purchased and licensed for the use made of it. Any software used must additionally not break the Conditions of Use of IT Facilities at LSE or the Jisc Acceptable Use Policy.

It is the responsibility of each user to ensure that any non-centrally-licensed software is legitimately purchased, deployed and used.

Software licenses that have not been used over the past 12 months will be redeployed.

## 2.4 Asset redeployment

LSE-owned IT assets – hardware, software, licences, cloud services – that are no longer in use must be returned to LSE for redeployment. This includes where the asset was purchased using research, departmental or divisional funds.

## 2.5 Non-compliance

All LSE IT Devices, as specified above, must comply with this policy. Breach of this policy may result in any device being remotely wiped, blocked from LSE's network, blocked from using LSE-provided services and software and may be considered a disciplinary offence.

## 2.6 Incident Handling

If a member of the School (staff or student) is aware of an information security incident that materially breaches this policy then they must report it to the Information Management and Technology Service Desk at IT.Servicedesk@lse.ac.uk or telephone 020 7107 5000.

If necessary, members of the School can also use LSE's Whistle Blowing (Public Interest Disclosure) policy (see http://www2.lse.ac.uk/intranet/staff/brightIdeas/haveYourSay/whistleBlowing/Home.aspx.)

## 2.7 Review and Development

This policy, and any subsidiaries, shall be reviewed by the Information Security Advisory Board (ISAB) and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations.

Additional regulations may be created to cover specific areas.

ISAB comprises representatives from all relevant parts of the organisation. It shall oversee the creation of information security and subsidiary policies.

The Information Security Manager will determine the appropriate levels of security measures applied to all new information systems

# 3 Responsibilities

**Information Management and Technology**

Provide the appropriate centralised IT asset management stores for the receipt of LSE IT Device information, as required by the legal, regulatory, contractual and licensing requirements outlined. Provision of client-based or clientless monitoring in order to extract such information.

**RLAB IT Manager**

Ensure the collection of RLAB IT Device information in accordance with the requirements of this policy.

**Global, Legal and Policy Division**

Responsibility for Information Asset Management policies.

**IT Device users**

Ensure their devices meet this policy. Report any breaches of this policy.

**IMT Information Security**

Responsibility for reviewing and maintaining this policy.

Technical

# Document control

## Distribution list

| Name | Title | Department |
|---|---|---|
| Information Security Advisory Board | | |
| Information Technology Committee | | |

## External document references

| Title | Version | Date | Author |
|---|---|---|---|
| Information Security Policy | 3.13 | 12/10/16 | Jethro Perkins |
| Conditions of Use of IT Facilities at LSE | 3.0 | 07/10/16 | Jethro Perkins |
| EU General Data Protection Regulation | | 2016 | |

## Version history

| Date | Version | Comments |
|---|---|---|
| 27/01/17 | 0.1 | Out for comment to: YL, PS, CA, JH, CR, SH |
| 31/01/17 | 0.2 | Updates as a result of comments. |
| 24/02/17 | 0.3 | Updated as a result of talking to IMT Customer Services |
| 14/03/17 | 1.0 | Updated according to ITC requests |

## Review control

| Reviewer | Section | Comments | Actions agreed |
|---|---|---|---|
| ITC | 2.4 | ITC required the policy to be “toughened up” with a more concrete commitment to redeploy School IT assets when they were no longer in use. | Section 2.4 included. |