1 Introduction

Data leaked from LSE-owned devices could lead the School to face:

- Investigation and a potential fine of up to £500,000 from the Information Commissioner's Office under the Data Protection Act
- Potential fine of up to 4% of turnover under the EU General Data Protection regulation
- Withdrawal or reassessment of contracts issued by research funders
- Reputational damage

One of the most common sources of data breach is through lost or stolen laptops. The ICO reported in 2012: "There have been a number of reports recently of laptop computers, containing personal information which have been stolen from vehicles, dwellings or left in inappropriate places without being protected adequately. The Information Commissioner has formed the view that in future, where such losses occur and where encryption software has not been used to protect the data, regulatory action may be pursued."[i]

As LSE conducts a large amount of research in the field, it is important that we provide *by default* a high level of assurance that, if a laptop containing research or other confidential data is lost or stolen, the data upon the device is not at risk of disclosure. This consequently helps protect the research and reputations of our staff and students, and the confidentiality and integrity of data assets we hold on behalf of funders, governments and other organisations.

Whilst in general LSE's approach is to affirm the responsibility of each user for the data under their control, in terms of how it is stored and accessed, laptop hard drive encryption is now an expected measure and therefore, like providing usernames and passwords, it should be included as default when a laptop is given to an end user.

LSE must therefore be able to control encrypt the hard drives of laptops before they are provided to users, in a manner that is for the most part transparent.

1.1 Purpose

To increase the default level of information assurance surrounding laptops owned by LSE and operated by staff and students.

To reduce the potential for fines from the ICO

To reduce the opportunity for accidental data leaks through loss or theft of laptops.

1.2 Scope

This policy applies to all LSE laptops built and owned by LSE, whether PC or Mac.

It will not be applied retrospectively to existing laptops.

[i] 'Our Approach to Encryption', *Information Commissioner's Office*, http://ico.org.uk/news/current_topics/Our_approach_to_encryption [Accessed 23/05/14]

2 Responsibilities

Members of LSE:
All members of LSE are responsible for treating confidential data appropriately, and according to LSE's Information Classification Standard.

All members of LSE are also responsible for reporting any incidents of non-compliance to the Information Security Manager.

IMT Information Security:
Responsible for this policy. Responsible for the storage and management of ad hoc encryption keys

IMT Systems Team:
Responsible for the encryption key management infrastructure, both for PCs and Macs.

IMT Support Teams:
Responsible for the implementation of hard drive encryption on PCs and Macs

Information Security Advisory Board
Responsible for the advising on and recommending information security policies to the Information Technology Committee, assessing information security risks, identifying and implementing controls to risks.

Information Technology Committee
Responsible for approving information security policies.

3 Policy

3.1 By default, laptop hard drives will be encrypted

When support teams build new laptops, the hard drives will be encrypted as part of the build process.

3.2 Encryption standards

Hard drives will be encrypted to AES-256-bit standard by default. Any deviation from this standard must be agreed in writing by the Information Security Manager.

3.3 Legal Requirements

LSE has a legal duty to provide encryption keys if requested under the Regulation of Investigatory Powers Act 2000. Consequently, full disk encryption recovery keys for LSE-issued laptops will be retained by IMT.

3.4 Opt-outs

Any individual wishing to opt out from having their laptop hard drive encrypted must have this agreed in writing by the Information Security Manager.

3.5 Compliance, Policy Awareness and Disciplinary Procedures

Failing to comply with this policy, LSE's Conditions of Use of IT Facilities or Janet's AUP may result in criminal or civil action against LSE.

Any breach will be handled in accordance with all relevant School policies including HR's disciplinary processes.

3.6 Further Policies, Codes of Practice, Procedures and Guidelines

This policy sits beneath LSE's overarching *Information Security Policy*. Other supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on LSE's website via the Information Security Policies, Procedures and Guidelines page. All staff, students and any third parties authorised to access LSE's network or computing facilities are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

3.7 Review and Development

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

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.

3.8 ISO27002 best practice controls governing the Laptop Hard Drive Encryption

A.7.1.3 Acceptable use of assets

A.7.2.2 Information labelling and handling

A.9.2.6 Secure disposal and re-use of equipment

A.11.6.1 Information access restriction

A.11.7.1 Mobile computing and communications

A.12.1.1 Security requirements analysis and specification

A.12.3.1 Policy on the use of cryptographic controls

A.12.3.2 Key management

A.12.5.4 Information leakage

A.15.1.3 Protection of organizational records

A.15.1.4 Data protection and privacy of personal information