Standard

Use of Cryptography

Information Security Manager

Document control

Distribution list

Name	Title	Department
Adrian Ellison	Assistant Director, Infrastructure Services	IT Services
Amber Miro	Assistant Director, User Services	IT Services
Andy Coulthard	Assistant Director, Management Information Systems	IT Services
Puneet Singh	Systems Manager	Technical Infrastructure Group, IT Services
Malcolm Barker	Network Manager	Technical Infrastructure Group, IT Services
Stephan Freeman	Information Security Manager	Technical Infrastructure Group, IT Services
James Hargrave	User Support Manager	User Support, IT Services
Tim Green	IT Manager	Library
Nic Warner	Computer Manager	STICERD
Kevin Haynes	Senior Assistant Secretary	Legal & Compliance Team

External document references

Title	Version	Date	Author

Version history

Date	Version	Comments

Review control

Reviewer	Section	Comments	Actions agreed

Table of contents

Introduction

Purpose

LSE does not have a centrally managed service to provide encryption. Therefore, there is a need to manage those installations of encryption software without incurring liability. This document covers the acceptable uses of encryption at LSE, the mechanism by which encryption products should be selected and the ways these products should be managed.

Scope

This document covers encryption in use on behalf of the School by individuals on either LSE-managed equipment or where LSE data is transferred onto personal equipment. It covers removable devices, local disk encryption and e-mail encryption.

This policy does not cover encryption used for securing web sites, password files or other “server-side” encryption.

This document will be superseded by a formal document on information handling, as part of the Information Security Policy suite.

Background

It is important to protect information held on electronic media from being either read or modified by unauthorised persons. A number of recent losses of data by the UK Government and its contractors have highlighted the issue.

Assumptions

Detail here any assumptions made (see Standard for Standards for details about what to include in this section).

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.

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.

Bullets

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

- Bullet
  - Nested bullet

Tables

Tables appear as follows:

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

Responsibilities

Individual users of encryption software are responsible for the adherence of this policy.

Line managers must approve purchase of encryption software.

IT Services must select and approve encryption software used to protect LSE data.

Individual user who intend to travel outside of the UK with encrypted data should check the legal status of encryption software and files prior to departure and waive any claims against LSE for issues relating to encryption software or encrypted files overseas.

Policy

Application

Data that contains personal information and where LSE is the Data Processor or Controller (as defined in the Data Protection Act 1998) must not be transferred to personal equipment or removable media unless with the express permission of the LSE's Data Protection Officer.

Sensitive or personal information sent over insecure networks should be encrypted in transit. This includes the use of e-mail encryption or VPNs when using the Internet to transfer data.

Information that is deemed to be sensitive by the supplying organisation or the departmental head processing the information must not be stored on personal equipment or removable media without the express consent of the information owner.

Sensitive or personal information stored on portable devices should be encrypted, using an IT Services approved encryption product.

Software selection

All encryption products should be FIPS 140 compliant and have achieved Common Criteria EAL2 compliance.

Where possible, a single software solution should be implemented and be approved and supplied by IT Services.

All e-mail encryption systems should be able to use the S/MIME standard for secure e-mail.

All VPNs should consist either of an IPSec tunnel or use SSL.

There must be a standard feature to allow all cryptographically secured files and e-mails to be encrypted against a default administrator key as well as the personal key of the user of the product.

Cryptographic Key Management

Minimum key lengths

For symmetric encryption, keys should be a minimum of 256 bits in length.

For asymmetric encryption, keys should be a minimum of 2048 bits in length.

Administration

Software products must be set up so that an administrator key can be used to access encrypted files in the event that the primary user of the software is unable to gain access to their encrypted data.

This administrative key shall be exported to a removable device and stored securely in the safe of the Information Security Manager. Access to this key will only be provided on production of a correctly completed form entitled "Request for access to

another user's data (e-mail and/or personal data storage [H: space] and/or voicemail)".

Compliance

The LSE has a requirement to be able to access all of the information it is responsible for at any time. In the event that a correctly authorised request is received to access information, either for regulatory purposes or otherwise, the School must be able to access encrypted data.

Therefore, all users of encryption products at LSE for use with LSE owned or managed data must agree and sign the declaration in Appendix A, that provides the authority for authorised LSE IT Services staff to access the unencrypted versions of data, held in encrypted form by individuals within the School.

Declaration

Declaration for the Use of Encryption Products at LSE

By using tools to encrypt or otherwise render information or data that I store unreadable except to me, I hereby accept the following:

- I will disclose any information, upon request and on receipt of a correctly authorised "Request for access to another user's data (e-mail and/or personal data storage [H: space] and/or voicemail)" form that is available from the Information Security Manager;
- I will allow LSE IT Services to securely keep a copy of the administrative key that will enable access to this data in the event that I am unable to;
- I will not store any information or data in encrypted form that would fall under the "**Legal Requirements and Prohibited Uses"** sections (7 and 8) of the Conditions for Use of IT Facilities;
- I will immediately alert IT Services in the event that I suspect that my access to my encrypted facilities have been compromised;
- I will enable a password-protected screensaver on the device that hosts the encryption software that automatically comes on within 15 minutes of being left idle;
- I will not share my passwords, either for my user account or the encryption software, with anyone;
- Any physical loss of devices holding encrypted or personal data will be reported to the Information Security Manager in IT Services and Security Manager in Estates as soon as possible;
- If I intend to travel outside of the UK with encrypted data, I will check the legal status of encryption software and files prior to departure and waive any claims against LSE for issues relating to encryption software or encrypted files overseas.

Name:

Department:

Signature:

Date:

Please send via internal mail to IT Admin Office, S167 (St. Clements)

Form created 10/12/2008

Glossary

Term	Definition
Information Owner	The person or organisation who has primary responsibility for the security of the information. This could be a 3rd party organisation, like The Home Office, or it could be an individual who's data is being used. In the context of the School, it is normally the person who created the information. It is not, normally, IT Services.
Symmetric encryption	Encryption where both ends of the communication channel have the same key to encrypt and decrypt.
Asymmetric encryption	Encryption where the sender encrypt to a recipients key and cannot access the data themselves once it has been encrypted. Keys are different at either end of the communication channel.
S/MIME	Secure / Multipurpose Internet Mail Extensions. A standard protocol for sending encrypted e-mail.
FIPS 140	Federal Information Processing Standard 140. A standard promoted by the US government for the minimum quality of data encryption algorithms.
Common Criteria	An initiative by the US National Institute of Standards and Technology and the National Security Agency to accredit products for varying levels of security using "EAL" levels. Higher EAL certification assures the user it should protect more sensitive information
EAL	Evaluation Assurance Level. Assigned to products through Common Criteria accreditation. They go from EAL1 to EAL 7.
VPN	Virtual Private Network. A term for creating a secure communications channel over an insecure network, like the Internet.
SSL	Secure Sockets Layer. A protocol for implementing a VPN.
IPSec	Internet Protocol Security. A protocol for implementing a VPN.

Sign off form

Library reference: ISM-SD-006
Use of Cryptography

Assistant Director, Technical Infrastructure Group: Adrian Ellison

Signed: ..... *Date:*.....

Comments: .....

Assistant Director, User Services: Amber Miro

Signed: ..... *Date:*.....

Comments: .....

Assistant Director, Management Information Services: Andy Coulthard

Signed: ..... *Date:*.....

Comments: .....

Systems Manager: Puneet Singh

Signed: ..... *Date:*.....

Comments: .....

Network Manager: Malcolm Barker

Signed: ..... *Date:*.....

Comments: .....

Information Security Manager: Stephan Freeman

Signed: ..... *Date:*.....

Comments: .....