1. Data placed on specialised file transfer systems (e.g. sFTP servers) will be deleted after a period of **72hrs**, unless
    a. specific business reasons,
    b. licence agreements or
    c. contracts

    require otherwise.

2.6 Physical Information Transfer

1. Information that is to be transferred via portable media: compact disc, DVD, usb flash drive, external hard drive etc. must either be
    a. stored on the transportation media in encrypted form (e.g. using file/archive encryption)
    b. or else the media must be encrypted (e.g. using BitLocker, VeraCrypt).
2. Any media containing confidential data using postal systems or couriers must be sent recorded delivery. Details for LSE's courier facilities can be found here: http://www.lse.ac.uk/intranet/LSEServices/postRoom/couriers.aspx

2.7 Physical Media Storage

1. If there are third party requirements for the original physical media to be retained, this must be kept in secure locked storage.
2. Otherwise, physical media must be either destroyed (e.g. compact discs, DVDs) or wiped (external hard drives, usb flash storage) using a secure eraser program (.e.g. 'Eraser') to US DoD standards (7 passes).

2.8 Phones

1. Do not leave messages containing confidential information on answering machines or call recording services
    a. these may be replayed by unauthorized persons,
    b. stored on communal systems
    c. stored incorrectly as a result of misdialling;

2.9 Fax machines

1. Unless explicitly and contractually required to do so, avoid transmitting any confidential data over fax machines.
2. Fax machines pose a number of high risks to the confidentiality, integrity and availability of confidential data, namely:
    a. unauthorized access to built-in message stores to retrieve messages;
    b. deliberate or accidental programming of machines to send messages to specific numbers;
    c. sending documents and messages to the wrong number either by misdialling or using the wrong stored number.

2.10 Internal information transfers

1. IMT operates a zero-trust network model, where internal communications cannot be assumed secure.
2. Therefore any internal system to system communication that includes or may include Confidential information must be encrypted to modern strong encryption standards.
3. Intra-system communication and system to system communication within logically-segregated "secure bubbles" does not have to be encrypted; appropriate security is applied at the boundaries

2.11 Encryption standards for server-side transport.

1. LSE uses the 'modern' list of ciphers contained in the Mozilla Foundation's server-side TLS documentation: https://wiki.mozilla.org/Security/Server_Side_TLS
2. All use of server-side information transfer facilities must meet at the least the 'modern' cipher list

2.12 Chain of custody

A clear chain of custody must be recorded for all confidential information transfers to or from third parties.

2.13 Review and Development

This policy, and its 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

2.14 ISO27001 Controls

A.13.2.1 Information transfer policies and procedures.

3 Responsibilities

Data Owners and Custodians

- Ensure all Confidential information is correctly identified.
- Ensure all Confidential information is transferred according to this policy, the applicable laws and contractual agreements.
- Ensure data is deleted according the requirements of the policy
- Ensure there are documented chains of custody for confidential information transfer with third parties

Department of Information Management and Technology:

- Providing encryption methods and programs
- Ensuring appropriate encrypted transport between internal systems, and between internal systems and Cloud systems
- Maintaining the External Collaborator Access Framework
- Providing access to appropriate information security functionality within Office365
- Maintaining deletion schedules on centrally-provided information transfer systems

Research Lab

- Responsible for providing secure transfer methods for RLAB users, in accordance with this policy.

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.

Document control

Distribution list

Name	Title	Department
Information Security Advisory Board		
Information Technology Committee		

External document references

Title	Version	Date	Author
Information Security Policy	3.12	06/10/16	Jethro Perkins
Information Classification Standard	3.0	15/03/13	Jethro Perkins
Cryptography standards server-side	1	16/03/16	Jethro Perkins
Encryption Guidelines	1	29/05/16	Jethro Perkins

Version history

Date	Version	Comments
	0.1	Initial version
02/12/16	0.2	Incorporating observations from the ISO27001 Project Board concerning the ingestion of data from third parties, and effective boundaries within secure systems or networks that render encryption unnecessary.
09/12/16	1.0	Approved by Information Technology Committee on 05/12/16. Moved to release version.

Review control

Reviewer	Section	Comments	Actions agreed
ISO27001 Project Board	1	Third party data once ingested would no longer fall out of scope	Policy updated
ISO27001 Project Board	1, 2.10	Confidential data within secure areas would no longer need to be encrypted in transit	Policy updated