1. Introduction

1.1. This information security policy document sets out principles and expectations about when and how encryption of University digital information should (or should not) be used. This is a sub-document of Information Security Policy (ISP-S1).

1.2. This document includes statements on:
   - Cryptography and UK law
   - Data encryption for secure network transit
   - Required use of encryption
   - Management of encryption keys
   - Required use of digital signatures
   - Unsupported use of encryption
   - Cryptography implementation

2. Related policies

2.1. Refer also to:
   - Information Handling Policy (ISP-S7)
   - Mobile Computing Policy (ISP-S14)

3. Cryptography and UK law

3.1. Export regulations relating to cryptography technologies are complex. (Any member of the University becoming involved in export of cryptography is advised to seek specialist advice. Information Assurance Services can assist by coordinating access to such advice.)

3.2. The Regulation of Investigatory Powers Act (RIPA) came into force in October 2000. Section 49 includes a provision for public authorities to demand, where it is judged there are reasonable grounds, decryption keys or decryption of information stored on computer systems in the UK. Anyone who could be assumed to have encrypted and stored data is very strongly advised to ensure that they retain the means to decrypt it.

4. Data encryption for secure network transit

4.1. Provided no other restrictions apply, it is permitted for all University staff and students to use computer systems which would normally and by default use encryption, in order to secure data in transit on a communications network.

4.2. Whenever possible and appropriate, encryption shall be used to support security of remote access connections to the University’s network and computing resources.

5. Required use of encryption
5.1. Loss, theft, or unauthorised disclosure of certain information could be detrimental to the University, its staff or students. Such information includes that defined as personal data by the Data Protection Act 1998. Where the University is handling digital personal data that cannot be sufficiently secured by physical controls, the data must be encrypted.

Data which must be handled securely, using encryption where pertinent, includes:

- Any personal data classed as “sensitive” by the Data Protection Act.
- Any data, that is not in the public domain, about a significant number of identifiable individuals.
- Personal data in any quantity where its protection is justified because of the nature of the individuals, source of the information, or extent of the information.

Data as described above must be encrypted:

- Where it is stored on a computing device or any computer storage medium which may be exposed to a significant risk of being lost or stolen. (Computers used to access remotely stored data or to process locally stored data may create cache files. Depending on the technology in use persistent and unencrypted cache files may be created.) Any such device when outside a secure University location is considered to be at significant risk, including home computers.
- Where it is to be transmitted via a computer network using a mechanism that does not itself incorporate encryption. Depending on the specific technology being used this could refer to: sending data by email either within or outside the University, transferring files offsite, remotely accessing files or Web pages. The risk is that unencrypted data in transit may be intercepted.
- Where the data is being sent using a postal service such that the data media could be lost, stolen or intercepted and read whilst in transit.

5.2. Where data being handled by the University is subject to an agreement with an external organisation specifying use of encryption, the agreed handling procedures, encryption technologies and standards must be used.

5.3. Where personal data is to be encrypted and no overriding requirements (from an external body) apply, the recommended minimum University encryption standards (or better) must be applied. For further details refer below to the “Cryptography implementation” section.

5.4. Individuals must be authorised by the Head of Department before taking or sending confidential information out of a secure University location. Optionally the Head of Department may elect to authorise specific individuals to routinely undertake a particular activity involving a specific type of data. A departmental record of such authorisations is to be established and maintained recording the following details:

- The data name or description.
- Who has been authorised to remove the data.
- Purpose for which the data is being removed.
- Date of data removal or an indication where removal is routine, e.g. “during exam marking”.
- Where the data is being taken or sent.
- Any agreed external security requirements that apply to the data.
- Confirmation that the data will be encrypted and handled securely.
- Encryption technology used e.g. name of encryption hardware or software.
5.5. University Web transactions that involve the transfer of personal, sensitive or confidential data or funds must use encryption, for example, Hypertext Transfer Protocol over Secure Socket Layer or Transport Security Layer (HTTPS).

6. Management of encryption keys

6.1. Departmental procedures must be in place:

- To manage encryption keys in a way that ensures encrypted stored data will neither become unrecoverable nor accessible by an unauthorised person.
- To facilitate authorised officers of the University to obtain prompt access to the encrypted information in the case of an emergency or investigation.
- To ensure that encryption keys are stored and always communicated securely.
- To record who holds encryption keys relating to important information.
- To revoke encryption keys when key holders leave.

6.2. Where practical, an unencrypted backup copy of critical University data should be securely maintained. Critical backup data should be stored where there are appropriate physical security measures in place (e.g. on resilient computer servers in an alarmed computer room or on backup tapes stored in a fire safe preferably in a different building).

6.3. Where University information received as email has been encrypted for secure transit, and is information which may be needed again later, it should be securely stored in a form which does not rely on ongoing accessibility of the senders public key.

7. Required use of digital signatures

7.1. Significant University business information being communicated electronically should be authenticated by use of digital signatures; information received without a digital signature should not be relied upon. Staff involved must assess the level of risk and decide whether to require use of digital signatures or whether to use an alternative means to authenticate the communication.

8. Unsupported use of encryption

8.1. Staff and students should:

- Not store encrypted data on University systems except where they are able to justify doing so for legitimate purposes.
- Be aware that the University reserves the rights to request sight, at any time, of the unencrypted version of any data stored on its systems and the option to remove any data.

9. Cryptography implementation

9.1. All encryption products, standards and procedures used to protect sensitive University data must be ones which have received substantial public review and have been proven to work effectively.

9.2. Where a department elects to undertake an activity that would incur a cost, in order to remain compliant with security policy, then that cost should normally be found from the departmental budget. For example, where a research project requires measures for secure data handling it is appropriate that costs for any necessary additional security measures are factored into the tender.
9.3. Further guidance about which encryption technologies are considered suitable for particular tasks and any supporting implementation details will be provided in policy sub-document:

- Cryptography Implementation (ISP-I7)

---

Failure to comply with University Policy may lead to disciplinary action.

The official version of this document will be maintained on-line. Before referring to any printed copies please ensure that they are up-to-date.