# Introduction to Data Encryption

1. Introduction ............................................................................................................. 2
2. What research data should be encrypted?.............................................................. 2
3. When should data be encrypted?............................................................................ 2
4. What data should be encrypted?............................................................................. 3
5. What encryption algorithm should be applied?....................................................... 3
6. Where can I find online Training?........................................................................... 3
7. Further Information................................................................................................. 4
1 Introduction
Encryption is a method by which data – digital or otherwise – is converted into an encoded form that can only be decoded and read if the user possesses an appropriate encryption key. It represents one of several techniques that may be applied to protect research data from unauthorised access.

2 What research data should be encrypted?

The need to protect data is mandated by the UK Data Protection Act 1998, which establishes the importance of applying “appropriate technical and organisational measures” to prevent “unauthorised or unlawful processing of personal data”. The DPA identifies two categories of information related to living individuals that require protection:

- **Personal data:** Information relating to a living individual that may be used to identify that person in isolation or in combination with other information sources. For example, their name and address.

- **Sensitive Personal data:** A sub-set of information on the individual is assigned special protection. This includes details of their (a) racial or ethnic origin, (b) political opinions, (c) religious beliefs or other beliefs of a similar nature, (d) trade union membership, (e) physical or mental health or condition, (f) details of sexual life, offenses or alleged offenses.

The Information Commissioner’s Office provides guidance and examples on applying the Data Protection Act in practice, as well as an overview of Key Definitions. The School’s policy in this area is outlined in the LSHTM Information Management and Security guidance.

3 When should data be encrypted?

Data that fits within the DPA categories should be encrypted for the entire period it is held. This includes:

- **Data at Rest:** Data held on storage media or computing devices should be protected to prevent unauthorised access. Protection measures should be applied to “ALL” copies of the data, including those held on back-up media.

- **Data in Motion:** Data being transferred from location A to location B should be encrypted to prevent it being intercepted and accessed. This covers electronic transfer (e-mail, FTP, etc.) and physical transmission (e.g. sending a USB disk through the post).

Encryption is only effective when a third party does not have access to the encryption key in use. If a user has already entered the password for an encrypted drive, but has left the machine powered on and unattended, data contained in the encrypted area may be easily accessed and copied by a third party.
4  What data should be encrypted?

Several options are available to protect personal and sensitive data using encryption:

- **Encrypt a disk in its entirety**: Full Disk Encryption may be applied in order to protect all data held on the drive.

- **Encrypt one or more partitions on the disk**: Personal and sensitive data can be held on the encrypted partition, while the anonymised material can be held on the un-encrypted partition.

- **Create an encrypted container**: A file that, when accessed using appropriate software, can be accessed and used in the same way as a physical drive.

- **Create an encrypted archive**: Compression software may be used to create an archive that can be accessed only by entering the correct encryption password.

Several software applications offer encryption functionality at different degrees of granularity. These include TrueCrypt, Microsoft Bitlocker, Apple FileVault, and 7-Zip, among others.

5  What encryption algorithm should be applied?

A simple rule to compare the security of different encryption algorithms is to find out the encryption key value size - an encryption key with a large number (e.g. 256 bits) is considered to be more secure than one with a smaller number (e.g. 128, 192 bits), making it less likely that a third party will be able to decode your data using brute force methods.

For health data, it is advisable to follow NHS Information Governance Guidelines to protect person identifiable and sensitive information, using an encryption algorithm that supports a minimum key length of 256 bits, such as AES 256, 3DES, or Blowfish.

6. Who can I contact for advice?

The LSHTM IT Services and RDM Support Service provide advice and guidance on use of data encryption tools

6  Where can I find online Training?

- Digital Curation Centre: Data storage and security training material inventory  
  <http://www.dcc.ac.uk/training/train-trainer/disciplinary-rdm-training/store/store>

- University of Edinburgh. MANTRA: Storage and Security: Online Learning Unit  
  <http://datalib.edina.ac.uk/mantra/storageandsecurity.html>
7 Further Information

- LSHTM Information Management and Security Policy and guidance
  < http://intra.lshtm.ac.uk/infoman/security/index.html >

- Information Commissioner’s Office. Data Protection Technical Guidance: Determining what is personal data.

- Cornell University. Encryption
  < http://www.it.cornell.edu/security/depth/practices/data_discovery/encryption/index.cfm >

- NHS Information Governance. Guidelines on use of encryption to protect person identifiable and sensitive information

- UCL Information Services: Data Encryption Good Practice
  < http://www.ucl.ac.uk/isd/common/cst/good_practice/encrypt >

- UK Data Protection Act 1998

- UK Data Service. Data Security
  < http://ukdataservice.ac.uk/manage-data/store/security.aspx>

- UK Data Service. Data Encryption
  < http://ukdataservice.ac.uk/manage-data/store/encryption.aspx>

- University of Minnesota. Encrypting Stored Data.
  < http://www.oit.umn.edu/security/topics/encrypting-data/ >