Guidance on storing sensitive data with BEAR Services

The Birmingham Environment for Academic Services (BEAR) is managed by IT Services and, amongst other things, provides resilient data storage replicated between two data centres held at the University, including backup storage to tape for disaster recovery. The data stored by IT Services is not encrypted so if you wish to store sensitive data* then there are some considerations to be made.

Use of BEAR DataShare (file synchronisation and sharing service)

Research Data that collects any personal information is subject to the Data Protection Act (DPA), which states that personal data must not be transferred outside the European Economic Area (the European Union member states plus Iceland, Norway and Liechtenstein), unless the country or territory to which the data are to be transferred provides an adequate level of protection for personal data.

Whilst we understand that many Cloud Services operate under the EU-US Privacy Shield scheme, the Information Commissioner's Office (ICO) has not yet advised on whether the Privacy Shield is sufficient for UK organisations to rely on. To be sure that your data storage is compliant with the DPA, the University recommends using BEAR DataShare where the data is stored in the UK at the University's data centres.

When applying for BEAR DataShare, you will be asked if you plan to store sensitive data. If you tick the box to say 'yes', we will then contact you to find out more and advise you to consider encrypting your data or at least password protecting it. Guidelines for storage of medical data which is patient identifiable should be provided by the Research Funder and usually require data encryption and/or pseudo-anonymisation, where a code is used to identify patients and the code is kept separate from the medical data. When you are working with medical data, please consult your local College IT Services team for advice on encryption and whether you can use BEAR DataShare.

Risk assessment of data encryption

The University provides guidance and policies on the use of encryption products on their IT policy and procedures webpage:
https://collaborate.bham.ac.uk/it/itas/Published/Guidelines/Guidelines%20-%20Encryption%20Products.pdf
(University login required)
If data encryption is not required by your Research Council or commercial funder, you may still choose to encrypt it if you wish to keep the data confidential.

Before you decide whether to encrypt your data, there are some risks to be aware of;

1) If the owner of the data loses the decryption key or password, then the data will be lost and cannot be restored from backups.
2) The encryption product used can affect how secure the data is.
3) Consider continuity of data access by securing a backup or escrow key (where an authorised third party can access the decryption key under certain circumstances). Please consult Legal Services for more information.
4) When data is stored on any central system, it is possible for system administrators in IT Services to be able to access your data. However, misuse of data or unauthorised disclosure would be a breach of contract and subject to University disciplinary procedures, therefore this risk is generally considered to be very low.

Some encryption products can be installed via the 'My Apps' link on your desktop (Windows only). If you are unsure on which encryption product to choose after reviewing the online guidance from IT Services, then talk to your local College IT Services team.

*Sensitive data could include commercially sensitive data and personal details, such as names and addresses, religious beliefs, medical conditions.

May 2017 Final