# Protecting Research Data

Introduction

The College recently commissioned an internal audit to assess the disaster recovery arrangements in research departments. The audit focused on data backup, recovery and the physical and environmental controls in place for research groups’ computer systems. The audit recommended that research departments should be made aware of relevant College policy relating to safeguarding and backing up data. This document provides a summary of relevant policy relating to safeguarding research data.

Identifying critical data

The security of research data is the responsibility of the computer system custodian and the PI responsible for the research grant. Industrial sponsors will often include confidentiality and availability clauses in contracts, which must also be considered by the PI. As a general rule, you should back up any data which if lost:

* would damage the research activities of your group
* could cause the College loss of reputation
* could result in loss of funding
* could result in breach of contract

Note that many research sponsors such as BBSRC, CRUK, MRC, etc., have formal requirements for data storage and also data sharing.

Data considered ‘sensitive’ should also be backed up. Sensitive data in the College is defined as any data which is covered by the Data Protection Act (any data identifying individuals, including patient-identifiable data) and commercially sensitive data.

Further information is available in the College’s Information Systems Security Policy relating to sensitive data and data backup.[[1]](#footnote-1)

Effective data backup and recovery practices

***ICT provide central file storage, backup and server hosting services.*** ***These should be used wherever possible, in preference to local arrangements.***

The central backup service provides secure, offsite data backup for College research servers, desktop PCs and laptops. Backup encryption is also available on request. Further details can be found on the ICT website.[[2]](#footnote-2)

Where data cannot be backed up using centrally provided services, the following principles should be observed:

* Any data identified as critical should be regularly backed up
* Backup data should be stored at an alternative location to the primary copy of the data
* Backup data stored on portable storage media (e.g. CD, DVD, USB data stick) should be kept physically secure (see below)
* Data backups should be updated regularly, depending on the rate of change of the data
* Backup copies of data should be checked regularly, to ensure they are accessible (e.g. not corrupt) in the event of recovery
* Data encryption must be used for backups of ‘sensitive’ data

*Physical data security*

When storing data it is important to ensure that it is held in a physically secure manner. When considering physical security, you need to address the security of premises, equipment and data:

* Ensure that computer systems are kept in a room which is locked when unattended
* Report suspicious persons loitering in secure areas to College Security
* Laptops and portable storage media should be encrypted if they hold valuable or ‘sensitive’ data
* Securely delete any valuable or ‘sensitive’ data on equipment before disposing of it.

Further information is available in the College’s Information Systems Security Policy relating to Physical Security of Information Systems[[3]](#footnote-3) and Disposal of Computer Systems[[4]](#footnote-4).

*Data sharing*

The College provides the SPIRAL repository (http://spiral.imperial.ac.uk) that is available to make documents and data publicly available. For researchers generating large volumes of data that is required to shared, this resource is not suitable and local arrangements must be made, in line with the research sponsors requirements.

If you would like further advice about protecting research data, and the services ICT can offer, please contact the ICT Service Desk (x49000, service.desk@imperial.ac.uk).

1. <http://www3.imperial.ac.uk/secretariat/policiesandpublications/informationsystemssecurity/> [↑](#footnote-ref-1)
2. <http://www3.imperial.ac.uk/ict/services/useremailfileanddirectoryservices/file_and_backup_services> [↑](#footnote-ref-2)
3. <http://www3.imperial.ac.uk/secretariat/policiesandpublications/informationsystemssecurity/codesofpractice/cop5> [↑](#footnote-ref-3)
4. <http://www3.imperial.ac.uk/secretariat/policiesandpublications/informationsystemssecurity/guidelines/guide11> [↑](#footnote-ref-4)