Information security and records management

What is information security?

Information security may be defined as the preservation of:

- confidentiality: protecting information from unauthorised access and disclosure;
- integrity: safeguarding the authenticity, accuracy and completeness of information and processing methods; and
- availability: ensuring that information and associated services are available to authorised users when required.

Appropriate protection is required for all forms of information, paper or electronic, to ensure business continuity and efficiency, and to avoid breaches of statutory, regulatory or contractual obligations.

Why is information security needed?

Organisations and their information systems face security threats from a wide range of sources, including computer-assisted fraud, sabotage, vandalism, theft, fire or flood. Damage caused by breaches such as computer viruses and computer hacking is becoming increasingly common and sophisticated.

Dependence on information systems and services means that organisations are increasingly exposed and vulnerable to security threats; security issues were not always the primary consideration in system design.

What does information security have to do with managing records

If you are managing your records properly, you should be keeping them secure. This process involves an assessment of how secure it needs to be, depending on the nature, content and importance of it. The Information Security Policy and the guidance on the Data Protection Act should help you to make this kind of assessment.

Information that will need to be kept secure includes:

- Personal information. For example student and staff information.
- Information relating to teaching and research, particularly prior to publication
- Information relating to the School’s commercial interests

As a general rule, if the loss or unauthorized access or editing of the information could cause damage to the School or stop you from doing your work, it will need greater security.

Storage of records

Where records fit into the categories listed above, they will need stricter storage solutions.

Paper records in these categories will need to be kept in lockable cupboards or drawers when not in use. This is particularly so when third parties have access to offices where records are stored. The Disability and Wellbeing Office have a good system in place for their paper records. A clear desk policy is recommended, where files and other paper documentation are locked away at the end of the working day.

Electronic records in these categories need to be kept password protected within databases or stored in a shared drive that the relevant people have access to. Cloud services should not be used particularly for personal information or information relating to the School’s commercial interests. Only put into the cloud what you can afford to lose. Portable storage devices should be encrypted or not used at all – the remote desktop allows access to information on the School’s systems and should be used whenever away from the School. A shortcut to the shared drive on your H space will allow access within the remote desktop connection. Keep antivirus software up to date on any laptops and password protect any mobile devices. Email is not a secure system, so be aware that confidentiality cannot be assured for any information sent via email.

Tracking of records

Tracking ensures that only those users with appropriate permissions are performing information tasks for which they have been authorised. Tracking systems can range from a handwritten note to an automated transaction in an electronic document management system. All tracking systems, however, have to meet the test of locating any record within the appropriate time period and ensuring that all movements are traceable. For example, the Exams and Ceremonies Office use an Excel based system for tracking scripts for Data Protection requests, allowing them to know where scripts are and when sent out and returned.

Electronic records and authenticity

Electronic records are particularly vulnerable to unauthorised or inadvertent change and loss. Security measures need to include:

- Digital signatures to protect the authenticity and integrity of electronic documents (the **Electronic Communications Act 2000** provides for legal recognition of electronic signatures and the process under which they are generated, communicated or verified).
- Scanning and storing electronic records and digitised documents according to BSI PD 0008:1999, *Legal admissibility and evidential weight of information stored electronically* to ensure their authenticity in the event of a legal challenge.
- Encryption of portable storage media.

Classification of information for security purposes

Classification of records is a shorthand way of determining how this information is to be handled and protected. Classifications should take account of business needs for sharing or restricting information, and the business impacts associated with such needs e.g. unauthorized access or damage to the information. The School's information security scheme can be found here. Please note, classifying information as confidential will not necessarily mean that it will be considered exempt from release under the Freedom of Information Act.

Destruction of confidential data

All staff have a responsibility to consider security when disposing of information in the course of their work.

For destruction of material in paper format refer to the guidance on paper records disposal.

Special care must be taken with the destruction of e-records, as deleted information can often be reconstructed. Erasing and reformatting disks or personal computers with hard drives which contained personal data is likely to be insufficient. Destruction should be carried out in collaboration with your IT Support team, which will have the software tools to ensure that the data is removed. Overwriting should ensure all previous information has been removed, but this should be executed by authorised staff only. All destruction should be carried out in accordance with the provisions of the relevant retention schedule for that information, allowing for an audit trail to be kept.