

The School depends upon the integrity of its computer based information and the availability of its information and communications technology (ICT) systems for its academic activity and administration. If these systems are unavailable or their information is compromised, teaching and learning may be disrupted, research delayed and administrative processes severely affected. To protect against these risks the School has developed this Information Technology Security Policy which seeks to ensure that all School ICT systems are secured against loss caused by inadvertent or malicious actions. Every member of the School should be aware of this policy and act in a way that is consistent with their responsibilities as set out.

Scope

The Information Technology Security Policy is applicable to all existing and proposed systems and is effective from the date of issue of this policy. This includes all computers, peripheral equipment, software and data located within the School or owned by the School but located elsewhere. The manager responsible for each system must ensure that all risks are identified and all reasonable measures are taken to guard against security breaches.

All members of the School, including staff, students, visiting academics and researchers must ensure that they comply with the requirements of the Information Technology Security Policy. Any suspected breaches of security must be notified to the appropriate IT Services, MIS or Library cluster support team who will notify the named individual(s) responsible for the particular ICT system(s) affected.

Physical Security

Computing devices, such as laptops, may only be connected to the School's network at designated connection points, (either cabled or wireless), or at another network point with the prior agreement of IT Services. Students who are resident in the Halls may connect their computers to designated study bedroom network points. Other computer and data communications equipment may only be connected by authorised support staff.

All equipment must be maintained in good working order and all reasonable steps must be taken to meet the manufacturer's operating guidance.

All equipment must be protected against fire, water, electrical fluctuations, physical damage and theft to an appropriate level commensurate with its replacement value and importance.

Access Control

With the exception of material intended for the general public, access to all ICT systems must be restricted to registered School users only. All activity involving the use of the School ICT systems or network must be capable of being traced to an individual.

School staff, students on a recognised course, applicants for courses who hold an offer, visiting academics, retired staff, alumni and other persons nominated by a senior officer of the School may be registered with a Username and password. Usernames must only be used by the person to whom they were issued and for the purpose for which they were issued.



Data and document owners must ensure that School information is protected against unauthorised disclosure, alterations or loss. All information must be backed up at a frequency appropriate to its importance. Sensitive information must also be protected against unauthorised reading and copying. This applies to information on personal computers as well as servers.

Responsibilities

The Library and Information Services Committee is responsible for the development and review of this Information Security Policy. The Librarian and Director of Information Services and the School Secretary and Director of Administration are responsible for ensuring that ICT managers implement the agreed policy.

The manager responsible for each ICT system must undertake regular risk analysis to ensure that all risks are identified and all reasonable measures are taken to prevent security breaches. The System Administrator(s) of each ICT system must ensure that the required security and access control policies are operative and effective and that the systems are maintained in line with current industry best practice.

Information owners and document creators must undertake regular risk analysis for each type of sensitive information or documents in their control and liaise with the appropriate ICT manager to ensure that the required protection mechanisms are in place.

All members of the School are responsible for ensuring that they guard against physical risks to ICT equipment and unauthorised access to ICT systems. Any actions which appear to contradict this Information Security Policy should be reported to the appropriate team. Where there is any doubt about who the appropriate team may be, it should be reported to the cluster support team who will notify the named individual(s) responsible for the particular ICT system(s) affected.

Advice and Guidance

The cluster support team can provide advice and guidance on most information security issues. Where necessary they will refer enquiries to other members of IT Services or MIS staff for further action.

This policy should be read in conjunction with the following supporting documents.

- The School Policy Statement on the Use of Information Technology
- Conditions of Use of IT Facilities at the LSE
- JANET Acceptable Use Policy
- The Security Handbook for System Administrators
- The Guide to Sensitive Electronic Information

Christine Cooper
April 20th 2002

