1

INFORMATION SECURITY POLICY

1. Introduction

The College is heavily dependent on information and information systems for all of its activities. The importance of the data, the systems used for processing and communicating data and the technological base on which these sit, make it essential that effective security measures are in place and observed. Electronic information and paper-based information are equally important. It is in the interests of all members of the College to ensure that effective security measures are taken for electronic and non-electronic data. This document is an information security policy based on the JISC Guidelines.

There is an obligation on the part of all individuals to take an active part in security. Security is only as strong as the weakest link, and can be ruined by individual actions (e.g. by leaving confidential papers accessible from an unlocked room, or leaving a computer accessible to others when it is logged into a confidential database). Individuals who do not play their part in security procedures place others and the College at risk.

1.1 Purpose

This policy sets out the responsibilities for information security, the steps that are to be taken to guard against risks and the action to be taken in the event of a breach of security.

1.2 Scope

The policy applies to all staff, students and other persons with access to College data and/or information systems.

The policy applies to all types of data (paper-based and electronic) and information systems. Those parts of the policy concerning electronic information or information systems have the authority of the Council Regulation concerning Information Technology.

1.3 Objectives

a. To assure all members of College that data they use:
   o is available and can always be accessed;
   o has integrity and has not been deliberately or inadvertently modified from an approved version;
   o is kept confidential i.e. sensitive information is only accessible to those authorised;
o can be produced in order to comply with legitimate requests from law enforcement agencies, from data subjects as defined by the Data Protection Act 1998, and in any other circumstances for which there is current or future legal provision.

b. To ensure protection against risks including but not limited to:
   o loss or damage to research or other academic work in progress or completed;
   o loss or damage to student work and projects;
   o loss or damage to College finance, personnel, student record information etc.;
   o damage to reputations caused by breaches of security;
   o liability for the consequences of breaches of security.

c. To ensure that members of the College are aware of their responsibilities and act accordingly

d. To ensure that College information systems are properly protected against security breaches.

As part of this policy it will be necessary to inform and educate all staff and students about the need for security as well as providing more specialised training and education for those who have responsibility for the IT systems.

1.4 Related Documents

Related documents include the Council Regulation concerning Information Technology, its associated Notes of guidance, and Guidance on computer security for staff and students.

2. Responsibilities for information security

The Principal has overall responsibility for overseeing the implementation of this policy in the College.

Heads of Departments/Schools, Institutes etc, i.e. controllers of significant budgets, are responsible for ensuring appropriate security (including physical security for access to rooms, filing cabinets and computers) is in place to protect data and information systems under their control and for taking action when appropriate. All departments need to have in place systems and procedures that protect the security of both paper-based and computer-based information, and mechanisms for responding and assisting in investigations in the event of a security breach.

The Director of ICT is responsible for ensuring appropriate security measures are in place for centrally provided IT-based teaching, learning and research systems, the IT infrastructure systems and the College-wide management information systems.

The Director of ICT will nominate two or more persons to form a central IT Security Team that is authorised to take charge in the event of any suspected or actual breach
The central IT Security Team will liaise with UKERNA's Computer Emergency Response Team (CERT) and other relevant security and law enforcement bodies, and will take such action or make such recommendations as are necessary for maintaining the security of the College's IT systems and networks.

All staff and students and other persons with access to information must take all precautions to protect data held in the College, adhere to the principles of the Data Protection Act 1998, ensure confidentiality of data is respected and observe any guidelines on information security that are issued by the College.

The Estates Department has responsibility to provide advice to Departments when considering the physical security of buildings and accommodation.

The Information Services Department has responsibility to provide advice and assistance to other members of the College when dealing with information held in electronic form.

### 3. Implementation of information security measures

Access to IT systems and provisions for disaster recovery should be managed in accordance with the Guidance on Computer Security for Staff and Students which is held on the College intranet at

http://qm-web.css.qmul.ac.uk/consultants/InfoSecPol/Guidance.html

Heads of Departments/Schools/Institutes etc should ensure that measures are in place to protect all information held in their respective areas. They should each nominate a suitable member of staff to take responsibility for advising on and implementing appropriate security measures in their areas. These persons will be known as Information Security Officers (ISOs).

The ISOs are responsible for ensuring that the information systems in their department are secured to a level appropriate for the information held on them and to a level appropriate for the importance and value of the systems themselves when considered as assets to the department. The ISOs will at least once a year carry out a risk assessment on all information for which they are responsible and take action to ensure that security measures are in place that are up to date and consistent with the risk assessment. They will consider all aspects of security including the physical security of equipment as well as systems security, access to data, and disaster recovery plans. Their review of security measures on the IT systems within their areas of responsibility will be in accordance with advice provided by the central IT Security Team.

The ISO or his/her nominees are authorised to carry out proactive monitoring and IT security audits within their local areas.

It is not expected that an ISO will have a systems management role for the information systems and/or data network in their department. However, security incidents involving electronic information systems require especially rapid action by technically competent personnel. Some departments/schools/institutes will have trained personnel but many will not; the central IT Security Team will provide the necessary technical expertise to assist the departments that do not have it.
However, given the devolved control and responsibility in the College for information systems, it is necessary that each ISO or his/her nominee should be able to assist the central IT Security Team rapidly in such cases and provide necessary access to the network infrastructure, computers, and accommodation areas containing them. They should be readily contactable to assist and take appropriate action to help investigate and rectify security breaches. There should also be alternative contacts in case of absence, and ideally 24/7 availability in emergencies. The central IT Security Team will maintain a list of these contacts.

NOTE: ISOs can be nominated to suit local situations, e.g. per department or shared between groups of departments or sections. They will be responsible to the nominating Head(s) of departments and must have clear authority for information security for the area they cover. ISOs may nominate specific technically competent individuals to act as contacts in the event of IT related incidents. These individuals must be registered with the central IT Security Team so that security breaches can be dealt with rapidly.

4. Breaches of IT Security

The risks associated with using IT systems connected to the Internet are considerable. The nature of current IT systems and network infrastructure is such that considerable damage can be caused very quickly. It is, therefore, essential that necessary actions can be taken quickly to limit damage and the extra requirements and responsibilities of the central IT Security Team and the ISO are aimed at achieving this when necessary.

Breaches of security affecting electronic information usually involve unauthorised access to one or more information systems, which may affect the security of the system itself. Any person suspecting a breach of IT security should report the matter immediately to their local ISO. Any ISO who becomes aware (or suspects) that any breach in IT security has taken place or been attempted should immediately inform the central IT Security Team who will work with the ISO or nominee to investigate the situation and if necessary carry out an appropriate course of action.

Where a breach of IT security has occurred a report on the investigation and action taken must be made to the Head of Department/School/Institute concerned and to the Director of Information Services. If the information included data identifying individuals the College Data Protection Officer must also be informed.

The central IT Security Team will also actively monitor the College network and periodically probe for security breaches and weaknesses in so far as is permissible under the Regulation of Investigatory Powers Act 2000. The team will follow up with such advice to the ISOs and action as may be appropriate. The central IT Security Team is authorised by the College to take such action as may be deemed appropriate anywhere on the College network, subject to the authority of the Director of Information Services and report to the relevant Vice-Principal and relevant Heads of Departments. This could include barring of access to the College network or the Internet, removal of access rights, impounding of equipment etc.
4. Dissemination

The Director of Information Services is responsible for ensuring wide dissemination of this policy.

5. Enforcement of Policy

Failure of an individual student or member of staff to comply with the terms of this policy may lead to action under the College Disciplinary Procedures. In the case of breaches of the policy that may constitute criminal offences or other infringements of law, the relevant law enforcement agencies or other bodies will be so informed.

July 2003