Faculty of Law: Information Security Policy

Introduction

The objectives of the Information Security Policy are to ensure that the confidentiality, integrity and availability of information in the Faculty of Law are preserved.

The Faculty of Law's computer and information systems underpin all of the Faculty's activities, and are essential to its teaching and scholarship. The Faculty of Law recognises the need for its members, employees and visitors to have access to the information they require in order to carry out their work and recognises the role of information security in enabling this. Security of information must therefore be an integral part of the Law Faculty's management structure in order to maintain continuity of its business, legal compliance and to adhere to the University's own regulations and policies.

Purpose

This information security policy defines the framework within which information security will be managed across the Faculty of Law and demonstrates management direction and support for information security throughout the Faculty of Law. This policy is the primary policy under which all other technical and security related polices reside. Annexe A provides a list of all other policies and procedures that support this policy.

Scope

This policy is applicable to and will be communicated to all staff (including academic staff based in colleges), students and other relevant parties including senior and junior members, employees, visitors and contractors. It covers, but is not limited to, any systems or data attached to the Faculty of Law's computer or telephone networks, any systems supplied by the Faculty of Law, any communications sent to or from the Faculty of Law and any data - which is owned either by the University or the Faculty of Law - held on systems external to the Faculty of Law's network.

Organisation of Information Security

The Dean is ultimately responsible for the maintenance of this policy and for compliance within the Faculty of Law. This policy has been approved by the Law Board and forms part of its policies and procedures.

The Dean and the Head of Administration and Finance will ask the Law Board to review this policy annually, to promote information security by keeping the policy up to date and by bringing it to the attention of Board members.

The Head of Administration and Finance, currently Charlotte Vinnicombe, is responsible for the management of information security and, specifically, to provide advice and guidance on the implementation of this policy. The Head of Administration and Finance is also responsible for conducting an annual risk assessment to identify information that is sensitive or confidential and may be stored in or transferred to a non-secure location.

In the St Cross Building, responsibility for the security of the IT infrastructure and network is shared between the IT Support and Database Officer, currently Bento de Sousa, and the University IT Services. In the Manor Road Building, where two Law Faculty research centres

are located, local IT infrastructure is the responsibility of the Manor Road IT Team. For more detail and the technical specifications, please refer to Annexe B, attached.

It is the responsibility of the Head of Administration and Finance to implement this policy and to ensure that all staff are 1) made fully aware of the policy; and 2) given appropriate support and resources to comply.

It is the responsibility of each member of staff to adhere to this policy.

Policy Statement

The Faculty of Law is committed to protecting the security of its information and information systems. It is also committed to a policy of education, training and awareness for information security and to ensuring the continued business of the Faculty of Law. It is the Faculty's policy that the information it manages shall be appropriately secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability of that information and to ensure appropriate legal, regulatory and contractual compliance.

To determine the appropriate level of security control that should be applied to information systems, a process of risk assessment shall be carried out in order to define security requirements and identify the probability and impact of security breaches.

Specialist advice on information security shall be made available throughout the Faculty and advice can be sought via the University's Information Security Team http://www.it.ox.ac.uk/infosec/infosecproject/ and/or OxCERT http://www.oucs.ox.ac.uk/network/security/.

It is the Faculty of Law's policy to report all information or IT security incidents, or other suspected breaches of this policy. The Faculty of Law will follow the University's advice for the escalation and reporting of security incidents and data breaches that involve personal data will subsequently be reported to the University's Data Protection Officer. Records of the number of security breaches and their type will be kept and reported on a regular basis to the Head of Administration and Finance.

Failure to comply with this policy that occurs as a result deliberate, malicious or negligent behaviour, may result in disciplinary action.

Signed: 

Date: 13/10/15

Position: Dean of the Faculty of Law

CLV 7 October 2015

S:\Information & website\Information Security\Information Security policy 2015.docx

Annexe A

I. University regulations and policies applying to use of University ICT facilities

This University has formulated rules, regulations and policies for the management of centrally provided IT and Communications facilities. These also comply with rules imposed by external bodies and are a condition of access to University facilities. All members, staff, students and visitors using the University's IT service, including the connection of any device to a departmental or college network connected to the University backbone network, must follow these regulations. Users must also be aware that many departments and colleges impose additional rules for use of facilities under their control.

II. Policies and procedures governing the use of University IT facilities in the Law Faculty

Information Security Policy

(a) Policy

The University Information Security Policy is available on the IT Services pages of the University website here:

- http://www.it.ox.ac.uk/infosec/ispolicy/

(b) Implementation

IT Services have written very detailed guidelines on all aspects of the implementation of the Information Security Policy, which are referred to as the 'Information Security Toolkit'. This is an extremely valuable resource for anyone wishing to understand particular aspects of Information Security, advising on best practice, and providing a range of possible solutions to technical issues.

The toolkit can be found on the IT Services pages of the University website here:

- http://www.it.ox.ac.uk/infosec/istoolkit/

University Statutes and Regulations

- Regulations Relating to the use of Information Technology Facilities

Rules imposed by external bodies as a condition of use

- JANET(UK) Statement of JANET acceptable use policy
- CHEST Code of Conduct for Site Licensed Software and Datasets

Other University rules with which users must comply

- Mobile Wireless Networking Regulations
- Rules for University Websites

- Advertising Material on University Web Pages
- Guidance on producing audio and video material for publication online
- Rules Regarding Mass Mailings
- Rules Governing JANET Access for Meetings, Conferences, etc Attended by Non-Members of the University
- Rules regarding Peer-to-Peer software
- Disposal of Computers within the University
- Guidelines for Handling Illegal Material.

If you suspect illegal material to be held within the University network you must report it to the Dean of the Law Faculty or to the Head of Administration and Finance, who will deal with it in accordance with these guidelines.

University Policy Statements

The University has issued the following policies for the use of ICT systems within the University. Responsibility for implementing these policies rests with all units (departments, faculties, colleges, halls) within the University. All users of the University's ICT facilities should be aware of these policies and local procedures to implement them, and must follow these as appropriate.

- University Policy on Data Protection
- Freedom of Information
- University Privacy Policy
- Trade Mark and Domain Name Policy

University Disclaimer of Liability

All services provided by the University are governed by this disclaimer.

- University Disclaimer of Liability

Training

All permanent staff and temporary staff employed for more than three months will undertake the 50-minute on-line Information Awareness Training module as part of their induction.

Incident reporting

Suspected or actual security incidents, e.g. the theft of loss of a mobile device, or a virus attack, should be reported immediately to the Head of Administration and Finance, Charlotte Vinnicombe, who will in turn report them to infosec@it.ox.ac.uk.

Annexe B

Description of IT infrastructure and technical specifications

The University of Oxford operates a devolved ICT structure in which responsibility for the management of computer systems and networks within departments and colleges rests with those departments and colleges. OUCS manages the backbone network, which connects departments, colleges and central services, and provides connectivity to the Internet through the UK Education and Research Network (JANET). Access for individual members is provided by the department and/or college to which they belong. All units are free to choose a model for implementation that best meets their individual needs in accordance with University policy.

In the Faculty of Law, decisions about access (physical access to premises, to paper files and to all computer files) are made by the Head of Administration and Finance, currently Charlotte Vinnicombe. IT access is facilitated and supported by the IT Support and Database Officer, currently Bento de Sousa. Some aspects of the website and on-line editing are facilitated and supported by the Web Development Officers, currently Catherine Donaldson and Steve Allen.

The file servers are directly managed by Bento de Sousa. He is responsible for securing all the local IT infrastructure, network, and equipment.

The faculty is connected to the University network via equipment that is located in the Bodleian Law Library and is managed by IT Services.

Further clarification is required for the management structure two centres in Manor Road and the HRFG project located at Pembroke College.

All college-based equipment purchased by the Faculty and used by Faculty staff is covered by the Information Security Policy of each individual college.