nuisance to occupants, except in designated residential study bedrooms;

(ii) prohibit smoking in University vehicles in accordance with the Smoke-free (Vehicle Operators and Penalty Notices) Regulations;

(iii) allow smoking in designated study bedrooms but not in any common area within residential buildings;

(iv) require occupants of the study bedroom to cease smoking (if requested to do so) to allow work to be carried out (cleaning, maintenance, etc);

(v) designate external areas where smoking is allowed. This is to allow a sensible approach to be taken to controlling smoking and associated waste.

(c) For full details of the policy see http://www.sussex.ac.uk/hso/

5. Administrative Regulations

(a) Students (other than part-time students not resident in the local area) must register under the National Health Service with a doctor in the University Health Service, or another doctor in the local area, by the end of the third week of their first term, and the name of the doctor with whom they have registered must be notified to the University Health Service by that date.

(b) No member of the University may use the name of the University (e.g. in a published letter or other document) in such a way as to give the impression that the University supports the views expressed in the publication, or any activities of the member, without the permission of the Registrar and Secretary. Any such publication must bear the name of the person responsible for it.

6. Regulations for the Use of Computers and Computer Networks

6.1 Information Security Policy

(a) It is the Policy of the University of Sussex that the information it manages shall be appropriately secured in order to protect the institution from the consequences of breaches of confidentiality, failures of integrity or interruption to the availability of that information.

(b) These regulations, together with subsidiary policies and implementation documents, comprise the University's Information Security Policy. It defines the framework by which the confidentiality, integrity, legality and availability of information within the University is ensured.

(c) The Information Security Policy will be regularly reviewed by the Information Services Committee or another body set up by Information Services Committee for this purpose.

Scope

(d) This policy is binding upon all users such as staff, students contractors, consultants, visitors and guests of the University when using University facilities, computers and/or networks, whether on site or via remote connections.

Implementation

(e) Information Services Committee has the authority to authorise and renew this policy.

(f) Information Services Committee may delegate specific responsibility for ensuring that the implementation documents and controls relating to information security are comprehensive, up to date and consistent with the law to another body set up for this purpose.

(g) The Director of IT Services may authorise access to private information for operational reasons. Exceptionally, the Registrar and Secretary may authorise legal access to users' private information to investigate suspected breaches of University Regulations or the law. Such actions will be reported annually in summary form to Information Services Committee. No one may access any other users' private information without explicit permission or authority.

Responsibility

(h) Users of University of Sussex facilities are responsible for protecting its information assets, systems and infrastructure. If you believe that information security has been compromised or is at risk you must inform the University by one of the methods outlined below.

(i) University Officers, Heads of Schools, Directors of Professional Services Divisions and Section Heads are responsible for ensuring that all information in their area is managed in conformance with this Policy. Risk assessments of information systems must be carried out and recorded to determine the probability and impact of security failures and the mitigation undertaken.

Discipline

(j) Students or staff who act in breach of this policy or who are negligent in their responsibilities to enforce it may be subject to disciplinary or capability procedures. In serious cases flagrant breaches of security policy may be grounds for exclusion from studies or for dismissal from employment.

Contact

All concerns about information security, whether or not communicated by other means, should be emailed to infosec@sussex.ac.uk or via the contact details at http://www.sussex.ac.uk/infosec/

Policy, Implementation and Advisory Documents

An up-to-date set of policy and supporting documents are available at http://www.sussex.ac.uk/infosec/

6.2 Regulations for the Use of Information and Communication Technology

Introduction

(a) These regulations define University's policy of acceptable use for Information and Communication Technology (ICT).

Purpose

(b) The purpose of these regulations is to ensure that the University's ICT systems are available for their primary purpose of supporting teaching learning and research. They also aim to reduce the risk of disciplinary or legal action by making users aware of the legislatory and regulatory framework in which the ICT systems must be used.

Scope

(c) This policy applies to all users of ICT equipment such as staff, students, contractors, consultants, visitors and guests.

(d) ICT facilities encompass (not exhaustively) Telephones, PCs, Macs, PDAs mobile telephones, wires and wireless (infrastructure), software databases, e-mail messaging, internet access, server access, owned, leased rented or otherwise provided when connected to the university infrastructure. For example, this means that if you use your own equipment connecting through the University network these rules will apply.

Note on Privacy

(e) The University of Sussex respects the privacy and academic freedom of staff and students. The University logs the use and operation of ICT systems to assure system performance and integrity. These logs are monitored but not routinely inspected. Within the terms of the Policy for Institutional Access to Information within University ICT Accounts, Equipment and Networks, the University has the right to access communications and data within its ICT systems for business purposes and for preventing, detecting or investigating crime or misuse of the system.

Acceptable Use

(f) University ICT systems are provided to support the advance of learning and knowledge through teaching and research. Occasional personal use that does not interfere with this primary purpose of the University is allowed.

(g) Most users will be issued with an account as part of student or staff induction. Other accounts may be authorised for specific purposes. Passwords to accounts must be kept secret.

(h) All hardware that uses the ICT systems must be registered here: http://www.sussex.ac.uk/its/roaming/ or installed by ITS or ICT staff.

Unacceptable Use:

Unlawful activity

(h) To access, create, change, store, download or transmit material which is threatening, offensive, defamatory, abusive, indecent, obscene or racist (other than in the course of properly supervised academic study and with the prior knowledge of the University).

(i) Intellectual copyright infringement – such as copyright trademark or patent.

(j) Accessing, deleting, amending or disclosing data or data structures without permission.

(k) Attempting to gain, or gaining, unauthorised access to ICT systems either within or external to the university.

Actions which threaten the ICT infrastructure

(l) Introducing viruses onto the network.

(m) Disrupting the network for example by activities such as port scanning, packet spoofing or denial of service attacks, or by excessive use of peer to peer applications (examples include Skype and Bit Torrent).

(n) Actions which put the security of information systems at risk.

(o) Wasting resources (time, networks or computers).

(p) Sending unauthorised bulk mail or 'Spam' and/or falsifying the authorship.

(q) Removing, damaging or tampering with any university ICT system.

Other unacceptable actions

(a) Offsite access to corporate data in an insecure manner:

(b) unsecured wireless links at home or internet cafes.

(c) devices not security patched and/or covered by current anti virus software.

(d) Storing private University information (for example confidential business information or personal data that is covered by the Data Protection Act) on portable computers or portable storage media without encryption.

(e) Unreasonable and excessive personal use that conflicts with the person's role in the University.

(f) Using the network for commercial gain without prior permission of the Director of IT Services.

(g) Not abiding by local rules relating to the area in which you are working/studying.

(h) Sharing computer accounts or loaning accounts or passwords to other people.

(i) The download, upload or use of unlicensed software (e.g. programs) or of multimedia objects (e.g. movies, games, music) in breach of copyright.

(j) Causing annoyance, inconvenience, offence, distress or nuisance to other users.

Sanctions

(k) Unacceptable use will be dealt with in a graded manner:

> (i) Where infringements are minor, computer resolution will be used – for example; excessive use of peer to peer software may result in the speed of your network connection being substantially reduced until resolved. This action will be performed by computer and no employee

of the University will become involved. Users may contact the ITS fault reporting service if they experience problems.

(ii) Where your actions put computing facilities at risk, your account and/or computing device could be suspended from the network, and your actions reported to your Head of School (students) or line manager (staff). The infringement may result in action being taken under staff or student disciplinary procedures as appropriate.

(iii) University policy is that criminal activity will be referred to the police.

7. Miscellaneous Regulations

(a) Lists of and links to other policies, procedures, codes of practice and regulations may be found on the Office of Governance and Secretariat website at:

http://www.sussex.ac.uk/ogs