IT Use Policy

21/08/2017
James Matthews

This policy sets out the principles for all IT users of the UUK Information Technology (IT) services and ensures compliance with good practice and statutory requirements.

1. Purpose and Scope

This policy covers access to computer equipment, software, operating systems, storage and file systems and network accounts providing access to Email, World Wide Web (WWW), File Transfer Protocol (FTP) and any other means of communication of a similar nature. Where individuals are not employees of UUK, but use the IT services, the service level agreement should be adhered to.

2. Policy Statement

2.1 UUK is committed to the development of its IT facilities to ensure a cost- and time-effective provision of its service.

2.2 UUK encourages all staff to use the IT facilities and the Internet in order to further the goals and objectives of their work, study or research.

2.3 UUK will encourage all staff to have the tools to optimise the systems provided.

3. Procedures

General

3.1Staff are representatives of UUK when using IT services. Actions therefore must be in the interest (and spirit) of UUK and not compromise UUK in any way or render it liable.

3.2 Staff must use UUK's IT services sensibly and appropriately (see Guidelines 4. 1 and 4.2) and in such a manner that it does not interfere with the efficient running of the organisation.

3.3 Personal system username and passwords or other security details will be issued to all staff and they must not be given to other staff, volunteers or external agents and no other login should be used. If someone else gets to know an individual's password, staff must ensure that it is changed or else obtain IT Support.

3.4 If PCs are left unattended without locking or logging off, the responsibility for any misuse of it rests with the individual.

3.5 Only software which has been approved by the Network Administrator can be used and must be in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

3.6 Staff must not attempt to gain unauthorised access to information or facilities, computers and services or to modify their contents. If access to information resources is needed, the Network Administrator should be contacted.

3.7 If information is being obtained or recorded about individuals staff must ensure that Data Protection legislation is not broken.

3.8 Staff must ensure that electronic media is treated as confidentially and as appropriately as paper-based material since it has the same legal status.

3.9 Data must be regularly maintained and deleted as soon as possible to reduce the storage burden on the server e.g. databases, emails etc.

3.10 Staff must not introduce viruses into the system and must check removable media (e.g. floppy disks, USB keys etc), even if they think they are clean (contact IT Support to find out how).

3.11 Use of facilities for personal purposes (e.g. sending and receiving personal email, and browsing the Internet) is permitted so long as such use does not:

- incur specific expenditure for Universities UK;
- impact on your performance of your job (this is a matter between each member of staff and their line manager);
- break the law;
- bring Universities UK into disrepute or make it contractually responsible;
- get used for accessing offensive or illegal material (see guidelines).

3.12 UUK reserves the right to monitor emails or internet usage to ensure that usage is in line with the policy, but will endeavour to inform an affected employee where appropriate. Valid reasons for monitoring may be when the organisation suspects that an employee has been viewing, sending or using inappropriate material, excessive usage, or where there is suspicion that information being seen is detrimental to the organisation. UUK reserves the right to retain information it has gathered for a period of 12 months.

3.13 Where staff use the IT systems inappropriately, facilities may be withdrawn by the Network Administrator. Deliberate and serious breach of this policy will be treated as misconduct/general misconduct and will lead to disciplinary measures which may include the offender being denied access to computing facilities or even dismissal.

3.14 Staff have a responsibility to read the latest version of this document which will be updated from time to time as needs dictate.

Internet

3.15 Staff must not trade insults with other people using the Internet or write, publish, look, bookmark, access or download obscenities or pornography or offensive material.

3.16 The organisation reserves the right to deny internet access to any employee at work although in such a case it will endeavour to give reasons for doing so. The Network Administrator may also block internet sites which are inappropriate.

Emails

3.17 Emails should be checked carefully and treated like any other form of written communication. What is normally regarded as unacceptable in a letter is equally unacceptable in an email communication.

3.18 Staff must not send messages from other people’s computers in the name of the user of that computer.

LOANS

3.19 Where equipment needs to be borrowed the Network Administrator must be contacted and details logged. For memory sticks, the Group Administrator should be contacted.

4. Guidelines

4.1 Examples of acceptable use include, but are not limited to:

- communicating with fellow employees, business or academic colleagues, clients or customers of Universities UK within the context of an individual’s responsibilities, work, study or research activities;
- acquiring or sharing information necessary or related to the performance of an individual’s responsibilities, work, study or research activities;
- participating in educational or professional development activities, meetings, seminars, conferences or workshops;
- general use for the purpose of extending or expanding an individual's personal knowledge or expertise in relation to their function within Universities UK;
- reasonable personal use for communication purposes, independent learning, access to public services etc.

4.2 Examples of Unacceptable Use include, but are not limited to:

- creation, transmission or downloading (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- creation or transmission or downloading of material that is designed or likely to cause annoyance, inconvenience or needless anxiety;.
- creation or transmission or downloading of material that could be interpreted as harassment, racially or sexually offensive and/or offensive to those with a disability;
- creation or transmission or downloading of defamatory material;
- transmission or downloading of material such that it infringes the copyright of another person.;
- deliberate computer tampering such as introducing malicious programs into the network eg, computer viruses or worms.;
- downloading of screensavers or games, interactive sounds, large graphic files and DVD products.

If in doubt it is prudent to remember the following quoted dictum that when using the Internet, you should not transmit anything that you would not shout in a crowded room or write on a postcard.