Information Technologies

Acceptable Use Policy

Date: 28 August 2012

Version: V3

1. Introduction and Scope

1.1. The College seeks to promote the effective use of information systems and related technology to facilitate a productive environment for learning and teaching. This Acceptable Use Policy (AUP) defines the general terms of acceptable use of computing resources. Computing resources are defined as computer hardware, storage devices or peripherals, computer software, network services, databases or information repositories and the contents of such systems.

1.2. The AUP is applicable to all users, including students, teaching staff, support staff and visitors. Any distinction in application of the policy between user groups is highlighted in the text. The document does not include procedural matters such as good practice or other descriptions which augment the policy. Where appropriate, these explanatory topics are covered by separate operational procedures.

1.3. Access to College information systems and computing resources is granted subject to the statements set out in the AUP in conjunction with student rules and regulations and, in the case of staff, contracts of employment. The policy applies whether these systems are used in standalone mode or connected to the College network and whether they are accessed on-campus or remotely. The policy also applies to non-College owned equipment (for example mobile devices) when connected to the College network. Visitors may only access College resources if authorised to do so.

1.4. All Internet access originating from the College network is in addition subject to the JANET Acceptable Use Policy, available at:

- www.ja.net/documents/publications/policy/aup.pdf ; and
- Abuse of the JANET AUP will be regarded as a contravention of this AUP.

2. Authorisation

2.1. Access to College resources is automatically available to all currently employed staff and registered students and will not be restricted on the grounds of disability, impairment or any other discriminatory category.

2.2. Users must correctly identify themselves at all times and must not masquerade as another or interfere with audit trails. Users should take reasonable precautions to protect their online accounts and other network resources.

2.3. When staff employment or a course of student study finishes, access to College computer systems will cease and user accounts will be closed.

3. Conduct and Misuse

3.1. Information systems and computing resources are provided primarily to support teaching, training, self-study and College administration. However reasonable personal use is also permitted provided it does not interfere with teaching or work commitments and complies with this policy.

3.2. It is expected that staff and students will act in a responsible and ethical manner and respect the rights of others when using College information systems.

3.3. The following acts will be construed as misuse and may result in disciplinary proceedings (for both staff and students):

- Storing or sending unacceptable material over College systems.
- Unacceptable material includes anything that is:
- Libellous, abusive, defamatory or malicious;
- Likely to promote illegal acts, goods or services;
- Obscene, indecent or pornographic;
- Racially, religiously, sexually or politically offensive;

- Likely to promote terrorism or violence;
- Commercially restricted or violates copyright, including pirated material; and likely to cause loss of business or reputational damage.
- Use of computer resources in a manner which is liable to harass, hinder, intimidate or cause offence to another person or group.
- Use of computer resources to commit fraud, deception or other criminal act.
- Vandalism or deliberate physical damage to College equipment.
- Unauthorised access to another user's (email, network, etc.) account.
- Impersonating another user whether real (via the user's account) or artificial (via 'doctored' data). For example, sending messages that appear to originate from another person.
- Sending chain or bulk ('spam') messages.
- Use of College systems for commercial gain, running a business, non-College related advertising or political lobbying.
- Using unauthorised or unlicensed software (including games, screensavers, plug-ins, add-ons, etc.).
- Introducing viruses or other malware (such as key loggers) designed to impact system performance, integrity, security, availability or harvest other's data.
- Causing denial of service or affecting system availability by congesting or disrupting College systems.
- Jeopardising the integrity, reliability or performance of College systems, software or data.
- Breaching or attempting to breach security controls.
- Contravening the JANET AUP.

4. Filtering and Blocking Content

4.1. Automated filtering systems are utilised to protect College information systems. These filtering systems cannot be guaranteed to provide absolute protection users should, therefore, treat messages from unknown sources with extreme caution.

4.2. For the safety of all users, especially young persons, the College makes use of automated systems designed to prevent access to content, data or programs considered unsuitable. This includes (but is not limited to) objectionable web sites which may host pornographic images and sites posing security threats. The extent of blocking will vary according to location. Additionally, access to certain network resources such as the Internet or software applications may be temporarily blocked.

4.3. It is unlikely that filtering and blocking systems will remove all unsuitable content, users must comply with the AUP by acting responsibly, ethically and legally.

4.4. Ultimately, responsibility for the suitability of information held on College systems lies with the owner/author. He/she must ensure that the material is appropriate for all recipients who might access it, including young persons. This particularly applies to content published on web sites, intranets, wikis, blogs or held in online teaching systems.

4.5. The College will take reasonable steps to block or remove material considered to contravene the AUP and if necessary will refer the matter to the police if it appears that a criminal offence has been committed.

5. Student Data Storage

The College provides networked storage facilities where students can save their work. Whilst every effort is made to ensure the integrity of storage systems, the College will not accept liability for loss of any student data stored on information systems, or consequences arising from such loss. All student data will be deleted at the end of the course of study. It is the responsibility of individual students who wish to retain data to ensure it is retrieved prior to deletion.

6. Monitoring and Privacy

6.1. In order to ensure that the educational objectives of the College are being fulfilled, and that computing resources are not being misused (as defined in this policy), the College reserves the right to monitor all aspects of the use of the network and to keep logs of individual user activity. The purpose of this monitoring is to:

- To prevent and detect computer viruses;
- Provide a traffic analysis, which will help to ensure the computer services are operating efficiently and effectively;
- To detect misuse of the College's computer systems; and
- To back-up data files to protect against hard disk failure.

6.2. Users should note that data held within network accounts or other resources (such as email) is not routinely inspected. User data will normally be treated as confidential and private. An examination will only take place in response to an allegation of AUP misuse or to investigate problems impacting the operation of the network and/or information systems. If necessary the College will access user account information and other files held on the computer systems for the purposes of investigating misuse or to preserve the integrity, security, availability and legality of the network. It should be noted that access/monitoring will not necessarily be notified to the user concerned. Such access may arise under the following circumstances:

- Requests for access/monitoring from Police or Security Services as allowed by current legislation;
- Requests made under the Data Protection Act (1998) and the Freedom of Information Act 2000 (Scotland 2002);
- Requests to establish facts as part of a misconduct investigation;
- Requests from the employee themselves; and
- To facilitate the operation, repair and essential maintenance of College systems.

6.3. The College recognises that it has a duty of care to respect the confidentiality of the data examined during such investigatory work.

6.4. To prevent disruption to normal College business, it may be necessary to grant access to data (including email messages and electronic files) belonging to staff (including agency contractors) that have left the College's employment, are on sick/absence leave or prolonged annual leave. Permission will always be sought before data is accessed. This will require the written authorisation from a member of the Executive Leadership Team.

7. Policy Enforcement & Advice

7.1. Each user has a personal responsibility to observe the terms of this policy. In most cases the College will prefer to inform users of a contravention of the AUP and will advise on any necessary corrective action. However repeated or serious contraventions will trigger the College's disciplinary procedures. This could result in various sanctions ranging from withdrawal of computing facilities to dismissal from the College or in extreme cases, criminal proceedings.

7.2. Whilst investigating an alleged policy contravention the College may take whatever action is deemed necessary to preserve evidence, including immediate withdrawal of user access to computer equipment and/or the College network.

7.3. The cost of a policy contravention investigation will be borne by the College however no liability will be accepted for user losses or expenses resulting from the withdrawal of access rights.

7.4. Any unauthorised action performed using computing equipment that exposes the College to possible litigation will be regarded as a breach of this policy. Where appropriate the College will seek reimbursement of consequent damages, costs or other expenditure awarded or incurred.

7.5. The co-operation of all students and staff is expected in order to guarantee a resilient and reliable College computing facility. Students who wish to report suspected computer or network abuse should contact their course tutor or a member of the Information Services Team. Staff reporting abuse should contact their line manager.

8. Legislation

8.1. All use of the College computer facilities must comply with existing UK legislation and EU directives.

8.2. The main laws covering use/misuse of College computer systems are :

- Copyright, Designs and Patents Act 1988;
- Malicious Communications Act 1988;
- Computer Misuse Act 1990;
- Disability Discrimination Act 1995;
- Data Protection Act 1998;
- Human Rights Act 1998;
- Regulation of Investigatory Powers Act (RIPA) 2000;
- Anti-Terrorism, Crime and Security Act 2001;
- Freedom of Information (Scotland) Act 2002;
- DDA 1995 (Amendment) (Further and Higher Education) Regulations 2006; and
- Equality Act 2010.

8.3. Contravention of these laws will be viewed as an automatic breach of this policy.

8.4. A full description of the relevant legislation can be obtained from the JISC Legal Information Service, available at www.jisclegal.ac.uk .

Approval Status	Approved by ELT pending approval by the Students, Staffing & Equalities Committee.	
Approved by		
Date Approved		
EQAI Status	Initial Screening Conducted? Full EQIA Conducted?	Yes: ☐ No: ☐ Yes: ☐ No: ☐
Proposed Review Date	January 2013	
Lead Department	Finance & Resources	
Lead Officer(s)	Vice Principal Finance & Resources and Information Technologies Director	
Board Committee		