Guest Wireless Access

Guide for Requesting Bulk Guest Wireless Access

Version 1.2

25th June 2009

Table of Contents

Requesting Bulk Guest Wireless Access

There are two methods available for requesting bulk guest wireless access:

1. Random Guest Wireless Access
2. Import Bulk Guest Wireless Access

Once you have requested the access please ensure the guest user has read and accepted the following polices, anyone breaching these terms will be disconnected immediately and further action will be taken.

- **Coventry University Code of Conduct for Use of ICT Facilities**

  This policy is included in this document but please ensure that you check http://www.coventry.ac.uk/cu/registry/general-regs/a/3643 for the most up-to-date policy.

- **JANET Acceptable Use Policy**

  This policy is included in this document but please ensure you check http://www.ja.net/company/policies/janet-aup.html for the most up-to-date policy.

Random Guest Wireless Access

To request usernames and passwords for a large number of guests for which details are not known in advance please raise a service request via the ITS Service Desk or your local IT support personnel requesting the number of accounts to be created.

The requester will be responsible for ensuring that the accounts are assigned to an individual and ensure that they have a record of username is being used by which guest accounts.

Imported Bulk Guest Wireless Access

To request usernames and passwords for a large number of guests please raise a service request via the ITS Service Desk or your local IT support personnel supplying a spreadsheet containing a complete list of all of the guests you wish to have created. Specifying the following details of the Guests:

- **First Name** (Mandatory)
- **Last Name** (Mandatory)
- **Organisation** (Mandatory)
- **Country Code** (Optional)
- **Contact Number** (Optional)
- **Email Address** (Mandatory)

As part of the service request also specify when the account should be valid from and to.

Example:

The following accounts should be valid from 09:00 on 1st January 2009 to 17:00 on the 5th January.

First Name	Last Name	Organisation	Country Code	Contact Number	Email Address
Joseph	Bloggs	ACME Ltd	44	07123 123456	jbloggs@acme.com
Jane	Doe	ACME Ltd	44	07123 123456	jdoe@acme.com

Please note that ITS will require 5 working days from receipt of completed details and RMS call to produce guest account.

Code of Conduct for Use of ICT Facilities

1. Purpose

The purpose of this Code of Conduct is to set the regulatory framework for the use of the University's Information Technology facilities. The University is connected to the UK academic network known as JANET, and abides by the regulations of use as described in the JANET Acceptable Use Policy (http://www.ja.net/company/policies/aup.html).

Any infringement of this Code will result in disciplinary action and may in addition be subject to penalties under civil or criminal law. Annex 2 sets out the criminal penalties which may follow the contravention of current legislation.

The terms used in this Code are defined in section 17.

2. Scope

This Code applies to all Users of ICT facilities which are owned, leased, hired or otherwise provided by Coventry University, ICT facilities connected directly or remotely to the institution's network and ICT facilities used on the institution's premises whether or not owned by the University, and used for any purpose whatsoever. It covers personal computers whether desktop or portable, PDA, mini or mainframe computers and computer networks, personal memory storage devices attached to University IT facilities; all software and data thereon and all computer based information systems, including telephones, provided for administrative or other purposes.

3. Basic Principles

All Users must act responsibly and guard against abuses that disrupt or threaten the viability of all systems. Every User is responsible for the integrity of the University's systems and must act in accordance with this Code, relevant law and contractual obligations and apply the highest standard of ethics.

Coventry University is committed to defending the principle of academic freedom and acknowledges that use of the Internet as defined in this Code is a very valuable contribution to the exercise of that principle. Without compromising this, Coventry University also aims to benefit from the Internet by presenting the University to the world.

4. Authority

The designated postholder with the authority to give access to ICT facilities and to give permissions as stated in this Code is normally the Dean/Director whose Faculty/School/Professional Service holds the inventory or asset register on which the relevant equipment is recorded. In the case of equipment on lease or hire to the University, it is the Dean/Director of the Faculty/School/Professional Service responsible for taking out the lease/hire agreement. For corporate information, it is the appropriate Information Custodian. Annex 1 lists the principal designated authorities.

5. Registration, Access Rights and Password Usage

Use of ICT facilities is conditional on prior registration with, and granting of access rights by, the appropriate Designated Authority, unless facilities are specifically exempted from the need for registration by the Designated Authority. Some activities may require the permission of more than one Designated Authority. Registration to use ICT facilities or the use of ICT facilities constitutes acceptance of this Code.

Users must notify the Designated Authority of any change in their status which may affect their right to use ICT facilities. This does not apply to students completing their studies, or a section of their studies, in the normal way.

The granting of access rights to some ICT facilities will be by the provision of user names and passwords giving access to locations, hardware and/or software ICT facilities. The provision of such user names and passwords by the Designated Authority will constitute authorisation

for the use of those ICT facilities for the purposes specified in the request for registration and under the conditions applicable to those ICT facilities.

Users must not use another user's name or password either with or without the account holder's permission, nor allow any password issued to them to become known to any other person, nor, having logged in, leave ICT facilities unattended and potentially usable by some other person.

Staff or students who are banned from using ICT facilities must not attempt to use those facilities whilst the ban is in effect. Other staff or students must not give access, nor assist with the giving of access, to facilities from which they know a person is banned.

Once a student or member of staff has left the University, all their permissions to use ICT facilities cease. Former staff or former students may only gain access to any ICT facility by reapplication in accordance with their new status.

6. Charging

The University reserves the right to charge for registration and/or for use of certain ICT facilities.

Users will be responsible for paying third party charges incurred through their use of ICT facilities (e.g. by accessing chargeable Internet facilities) unless an alternative payment mechanism has been formally agreed in advance with the Designated Authority. Where a payment mechanism has been agreed, users must still ensure they take reasonable care to limit charges incurred by the University. Users will be responsible for paying excessive charges whether caused deliberately or by negligence.

Users will be liable for the cost of remedying any damage they cause to the ICT facilities or to remote systems.

7. Non-Institutional Use

Use of ICT facilities (including email and the Web) by staff for personal purposes during their normal working hours is prohibited. However, personal use of email and the Web by staff outside their normal working hours is permitted provided that it is reasonable, does not breach this Code of Conduct, does not incur other University resources or impinge on other users, and does not in any way implicate the University. Such use may be subject to charge.

The use of ICT facilities for commercial gain must have explicit written prior permission, in accordance with University procedures for the carrying out of commercial work.

The use of ICT facilities to the substantial advantage of other bodies such as employers of placement students must have the explicit written prior permission of the Designated Authority and may be subject to charge.

Use of ICT facilities by persons other than staff or students must have the explicit prior permission of the Designated Authority in consultation with the Director of Marketing and Communication. and may be subject to charge.

Use by staff of the University's telephone system for chargeable private calls is prohibited except in the case of a local call home to notify family of an unexpected delay due to official business, or the occurrence of a serious family emergency which necessitates your contacting home, or where express permission has been given by the appropriate line manager. Use by students of the University's telephone system is prohibited, except where explicit permission has been given by an appropriate member of staff.

8. Monitoring

Coventry University retains the right to monitor use of all its facilities at any time without notice to ensure they are not being misused or University regulations breached. This monitoring will include the use of software that keeps a log of web sites accessed. In the case of ICT facilities, access to some web sites may from time to time be blocked.

The University also seeks to prevent receipt of inappropriate material by checking e-mail traffic automatically, rather than by the more intrusive (but also more accurate) means of

checking the content of individual e-mail messages by human intervention. As a consequence, some e-mails may be mistakenly labelled by the automated process and all staff are asked to make allowances for this possibility.

Moreover, Coventry University is committed to responding promptly to any potentially damaging publication (including email) by withdrawing from its services any unacceptable materials and taking any other necessary action. This may mean that users responsible for such materials have their access to the University's ICT facilities withdrawn pending disciplinary action. A suspected infringement of this Code may also lead to withdrawal of access to facilities pending investigation.

Where it is suspected that material displayed, stored or transmitted on University ICT facilities may risk criminal prosecution or civil legal action, or that material, even if legal, is not considered appropriate for publication or transmission by the University, the Vice-Chancellor or a Pro-Vice-Chancellor may authorise the Director of IT Services (or his/her nominee) to take appropriate action. This may involve isolating a server to its local subnet on the network until the offending material is removed or revised or the confiscation of the personal computer involved.

During routine systems administration (eg redirection of undelivered mail) or in the event of systems problems (eg hardware or software failure or attacks by hackers), staff who maintain the central and local ICT facilities are authorised to look at any information or files necessary to deal with the matter and/or to protect the systems and the information they contain. Such staff are required to treat any information they might see which is unrelated to the problem as strictly confidential, save where the information is such that it may constitute a breach of this code.

Monitoring of the activities of individual students in a classroom situation for academic purposes may also occur.

Targeted covert systematic monitoring or investigation of a user is subject to authorisation by a designated authority. Where the User is a student the designated authority is the Registrar and Secretary or, in his/her absence, the Assistant Registrar (Legal Services) or the Director of IT Services. Where the User is a member of staff the designated authority is the Director of Human Resources or, in his her absence, the Deputy Head of HR Systems and Reporting or the HR Operations Manager.

Such authorisation must be obtained in advance save where time is of the essence and the seeking of authorisation may involve a significant risk of system damage or loss of evidence. In such cases, the circumstances and the action taken shall be reported to an appropriate designated authority as soon as practicable thereafter.

Billing information on the use of the University's telephone system will be sent to Deans/Directors or their nominees (eg Resource Managers).

9. Security

It is the responsibility of all staff and students to comply with the University's Information Security Policy and its supplementary documents. The Information Security Policy can be found at http://www.coventry.ac.uk/cu/its/userinfo/security.

10. Equipment

Users are responsible for ensuring that they are sufficiently familiar with the operation of any equipment they use to make their use of it safe and effective, and to avoid interference with the use of it by others.

Equipment or other ICT facility which is normally fixed may NOT be physically moved without the prior agreement of the Designated Authority.

No equipment may be connected in any way into any network, workstation, or other ICT facility without the prior written agreement of the relevant Designated Authorities. Permitted connections must comply with any published policies and procedures.

Where ICT equipment is allocated to an individual, that person is responsible for the care of that equipment and its safe return on request.

11. General Use of Facilities

Use of the University's ICT facilities is governed by both the University's regulations and by legislation and other external requirements. Where a particular piece of legislation or an external requirement applies, this is indicated. Further information about relevant legislation can be found in Annex 2 to this Code of Conduct.

Users must:

- respect published times for access to ICT facilities;
- abide by the regulations of use as described in the JANET Acceptable Use Policy (http://www.ja.net/company/policies/aup.html);
- use the University's ICT facilities and information resources, including hardware, software, networks and computer accounts, responsibly and appropriately;
- respect the rights of others and conduct themselves in a manner that does not interfere with or cause offence to others and not engage in any activity which denies reasonable services to others or wastes staff effort in dealing with the consequences;
- adhere to the terms and conditions of all licence agreements relating to ICT facilities which they use or have access to, including software, equipment, services, documentation and other goods;
- abide by the terms and conditions of the various operating policies issued and approved by the Vice-Chancellor;
- observe operating policies issued by the relevant Designated Authority;
- when using networks and remote ICT facilities comply with any published rules for their use;
- take every precaution to avoid damage to equipment;
- take all reasonable precautions to prevent the introduction of any virus, worm, Trojan horse or other harmful or nuisance program or file into any ICT facility;
- be mindful of the risks of crime and report suspicious activities to the Designated Authority or the Protection Service;
- use all consumables, including stationery, for the purpose for which they were supplied and as far as is reasonably possible minimise consumption;
- dispose of unwanted paper output to minimise fire risk;
- arrange back-up copies of their own work if required. This might be achieved by using services provided by the institution;
- ensure they start and terminate each session of use of ICT facilities in accordance with published instructions;

Official Secrets Acts 1911-1989

- ensure that any material which relates to security, intelligence, defence or international relations is securely stored and is not displayed on the University's computing facilities;

Defamation Act

- ensure that all published facts are accurate;
- ensure that opinions and views expressed electronically do not discredit their subjects in any way which could damage their reputation;
- obtain written approval from their Dean/Director if it is felt that material might be potentially defamatory before publishing or transmitting such material;

Data Protection Act

- only use personal data for a University-related purpose;
- ensure that the use of University-related personal data is restricted to the minimum and is consistent with the achievement of legitimate purposes;
- contact the University's Legal Compliance Officer before conducting any activity which involves the collection, storage or display of personal data through the University's computing facilities.

Users must not:

- cause any form of damage to the Institution's ICT facilities, nor to any of the accommodation or services associated with them. Smoking, eating or drinking in any student ICT facility room is strictly forbidden;
- modify any software or incorporate any part of provided software into their own work without permission from the Designated Authority which must only be given where this is permissible under the current licence agreement;
- deliberately introduce any virus, worm, Trojan horse or other harmful or nuisance program or file into any ICT facility, nor take deliberate action to circumvent any precautions taken or prescribed by the institution to prevent this;
- delete or amend the programs, data or data structures of other users without their permission;
- in their use of ICT facilities exceed the terms of their registration or any other terms made aware to them by the Designated Authority subsequent to registration, or breach in any way the University's academic or general regulations;
- download, store, create, display, print, produce, circulate or transmit (other than for properly supervised and lawful research purposes) offensive and/or harassing material in any form or medium, or material which is designed or likely to cause annoyance, inconvenience or needless anxiety (such as chain emails);
- make any material available externally, whether by transmission or by loading on externally accessible systems, that is liable to damage the reputation of Coventry University;
- post damaging or offensive messages attacking staff or other students on social networking sites such as RateMyProfessors, MySpace, Facebook or YouTube;
- alter access rights to filestore directories or within Outlook/Exchange in such a way as to allow others to breach the Code of Conduct, or to circumvent quota or access restrictions;
- interfere with the use by others of ICT facilities nor remove nor interfere with output belonging to another user;

Computer Misuse Act

- display any information which enables others to gain unauthorised access to computer material (this includes instructions for gaining such access, computer codes or other devices which facilitate hacking);
- display any information that may lead to any unauthorised modification of computer materials (such modification would include activities such as the circulation of "infected" software or the unauthorised addition of a password);
- display any material which may incite or encourage others to carry out unauthorised access to or modification of computer materials;

Copyright, Designs and Patents Act

- create, make available, store or transmit on the University's computing facilities material (such as software, video, music) that infringes the copyright of another person or company;
- install, use or assist others with the use of Peer-to-Peer file sharing applications which infringe the copyright of another person or company;

Terrorism Act 2000

- participate in any form of interference or disruption of an electronic system;

Defamation Act

- place links to bulletin boards which are likely to publish defamatory materials;

Obscenity legislation

- access, disseminate or encourage access to materials which the University deems to be obscene, pornographic or excessively violent through the University's computing facilities;

Discrimination legislation

- use the University's computing facilities to place or disseminate materials which discriminate or encourage discrimination on grounds of age, gender, sexual orientation, race, disability, religion and belief;

Criminal Law

- place links to sites or bulletin boards which facilitate hacking and activities of a similar nature;
- place links to sites or bulletin boards where copyright protected works, such as computer software, are unlawfully distributed;
- place links to sites or bulletin boards which display pornographic materials;
- place links to sites or bulletin boards which are likely to contain discriminatory statements;
- engage in or promote any terrorist activity;
- use keyloggers or similar devices whether physical or software based for unlawful purposes.

JANET Acceptable Use Policy

- transmit any unsolicited commercial or advertising material through the University's computing facilities other than advertising in connection with specific mail lists where the advertised products or services are pertinent to the purpose of the list;
- disseminate any information concerning courses or facilities provides by the University or any other advertising material which is not "legal, decent, honest and truthful" and therefore in contravention of the Code of Practice for Advertisers issued by the Advertising Standards Authority.

12. Publishing on the World Wide Web

Publishing on the Web enables the University to make an immediate and far reaching impact on an ever-increasing audience. It is therefore essential that every effort is made to ensure that the material displayed is of the highest standard. Publishing guidelines are available from Marketing and Communications.

Only material related directly to the University, or to the academic research and consultancy interests of Faculties/Schools/Departments/Units can be published. The responsibility for all materials rests with the Custodian in the first instance.

All materials published on the University's Web servers which do not belong to the category of Web pages of individuals (see Section 13 below) must carry the name and e-mail address of the Provider and Author and the date on which they were produced, together with an expiry date where applicable;

(The above information may be contained in a META tag rather than displayed on the Web page itself)

All web sites must be agreed by Marketing and Communications and the only domain name permitted is coventry.ac.uk/.

All design and marketing work (including promotional material) must comply with the brand guidelines and must be signed off by Marketing and Communications.

All external supplier usage for marketing must be with agencies or organisations authorised by Marketing and Communications, and by Purchasing, to the corporate agreed terms.

13. Web Pages of Individuals

Staff are permitted to have individual Web pages for legitimate University purposes, as approved by their Dean/Director.

Students currently enrolled on research programmes (but not taught postgraduate programmes), are permitted to have individual Web pages, but only for academic and research purposes. Permission must first be obtained from the Custodian in their area. Similarly, it is recognised that as part of their academic programmes, some undergraduates and postgraduate (taught programme) students are required to produce a Web page for a

time-limited period. Again, it is the Custodian's right to delegate custodianship to a named individual (course tutor, programmes manager) for this purpose.

14. Retention

Users' data and software will be subject to published procedures for their removal or archiving after specified periods. Users' outputs are disposed of after published periods, if not collected.

15. Disclaimer

Coventry University accepts no responsibility for the malfunctioning of any ICT facility or part thereof, whether hardware, software or other nor for the loss of any data or software or the failure of any security or privacy mechanism.

No claim shall be made against Coventry University, its employees or agents in respect of any loss alleged to have been caused whether by defect in the resources or by act or neglect of the Institution, its employees or agents.

16. Infringement

Any infringement of this Code constitutes a disciplinary offence under the applicable procedures for students and staff and may be treated as such regardless of legal proceedings. Sanctions include withdrawal of access to ICT facilities and, where appropriate, dismissal or expulsion.

Users must provide full assistance to authorised members of staff carrying out enquiries on behalf of the University into suspected infringements of this Code.

17. Definitions/Responsibilities

The terms listed below have within this Code the meanings given for each.

Institution: Coventry University.

Designated Authority*:* The designated post-holder with the authority to give access to ICT facilities and to give other permissions as stated in these regulations, or person with delegated authority granted by the designated post-holder (see Annex 1).

Staff*:* Persons employed by Coventry University, whether academic, administrative, technical or other. These include full-time, part-time, and contractors for the duration of their contract.

Student*:* An individual enrolled or registered with the institution or undertaking study of any kind provided by, at or under the auspices of the institution.

User*:* Anyone using or accessing, for any purpose, any kind of computer hardware or software that is either provided by the University, or is used or accessed from premises owned or leased by the University.

Information Custodian*:* In order to assist with the appropriate use of University information, certain types of information have an Information Custodian associated with them. The Information Custodian is responsible for setting the rules governing the University's use of that type of information, subject to University policies.

Provider*:* A Provider is responsible for:

- the provision of data called for by a Custodian following the delineation of a data set;
- ensuring that the procedures set by the Custodian in respect of data collection are followed;
- ensuring the accuracy of the data at their source;
- ensuring that additions, updates and amendments are carried out as required and permitted by the Custodian.

A Provider may belong to the same academic or professional service as the Custodian to whom s/he supplies data but equally well may be based elsewhere in the University. The mapping of Custodians and Providers is clearly many-to-many.

A Provider may well collect data from a number of people and sources but the responsibilities given above will rest with the nominated Provider. Each quantum of data supplied to a Custodian will carry the name of the Provider and be dated so that queries can be directed and answered quickly.

***User name**:* A code issued by a Designated Authority to an individual, which is subsequently used to access appropriate ICT facilities.

***Damage**:* Any deliberate or accidental damage to any ICT facility or University property, including any modifications to hardware or software (including data) which incur time or cost in restoring the system to its original state.

***The Internet**:* The term used to describe the complex interconnection of a vast array of international computer networks. Various methods, or protocols, exist to enable users of those computers to exchange information.

***The World Wide Web**:* Often referred to as WWW or just Web, provides the protocols which allow Web clients to access the Internet.

***PDAs**:* Personal Digital Assistants are small portable handheld computers that organise data such as address books, schedules, calendars and task lists. PDAs are also capable of acting as a mobile phone and can work with a desktop PC.

***Personal Memory Storage Devices**:* These are high capacity storage devices often referred to as 'pen-drives' or 'memory sticks'. They are usually USB connected and are usually used to port data between systems or to secure data.

Annex 1 - Principal Designated Authorities

The designated authorities for University equipment are as follows:

The campus-wide voice and data communication network - Director of IT Services

Centrally managed ICT facilities - Director of IT Services

Faculty/School ICT facilities - Dean of Faculty/School

Professional Services ICT facilities - Director of holding Service or Director of IT Services (as defined by standard rules in section 4)

Telephone handsets – Dean of Faculty/School, Director of Professional Service or VC/PVC

Annex 2 - Legal and related requirements

Computer Misuse Act

The Computer Misuse Act was introduced in 1990 to secure computer material against unauthorised access or modification. Three categories of criminal offences were established to cover the following conduct:

Unauthorised access to computer material (basic hacking) including the illicit copying of software held in any computer.

Penalty: Up to six months imprisonment or up to a £5,000 fine.

Unauthorised access with intent to commit or facilitate commission of further offences, which covers more serious cases of hacking.

Penalty: Up to five years imprisonment and an unlimited fine.

Unauthorised modification of computer material, which includes:

- Intentional and unauthorised destruction of software or data;
- The circulation of "infected" materials on-line;
- An unauthorised addition of a password to a data file.

Penalty: Up to five years of imprisonment and an unlimited fine.

Copyright

Staff should refer to the Staff Handbook for clarification on copyright ownership of their work.

The Copyright, Designs and Patents Act 1988 is applicable to all types of creations, including text, graphics and sounds by an author or an artist. This will include any which are accessible through the University's computing facilities. Any uploading or downloading of information through on-line technologies which is not authorised by the copyright owner will be deemed to be an infringement of his or her rights.

Please note that the application of the Copyright Act to electronic copying is even stricter than its application to photocopying, since the fair dealing arrangements which usually apply to libraries (ie one article per journal for the purposes of research or private study) do not exist for computerised materials.

Some types of infringement give rise to criminal offences, the penalties for which may amount to up to two years' imprisonment or an unlimited fine. It is also possible for the copyright owner to claim compensation or to have infringing activities prevented by an injunction.

File Sharing

You must not make available by any means (including, but not limited to, web server or P2P file-sharing software), any material unless:

- you are the copyright holder, *or*
- you have a licence to make the material available, *or*
- the material is in the public domain.

Terrorism Act 2000

An attack on any electronic systems can be classed as an act of terrorism as well as a criminal offence. What constitutes an attack includes hacking websites or blocking websites, with a political agenda or public intimidation in mind.

Data Protection

The Data Protection Act 1998 concerns information about living individuals which is processed both automatically and manually. It basically gives rights to those individuals about whom information is recorded, and demands good practice in handling information about people.

With a few exceptions, every person or organisation holding personal data (data controller) must lodge a notification outlining their use of personal data with the Information Commissioner. Coventry University is registered as a data controller. Any use of personal data beyond the description stated in the University's notification will be illegal. In order to find out whether your proposed use complies with the University's notification contact the University's Legal Compliance Officer in the office of the Registrar & Secretary.

In addition, data users must comply with eight Data Protection Principles established by the Act. The Data Protection Principles are intended to protect the rights of the individuals about whom personal data are recorded. Guidance as to compliance with the principles may be obtained from the University's Legal Compliance Officer.

The new Act extends the protection given to computerised information to manually stored data. It also prohibits the transfer of personal data abroad to countries which do not provide adequate protection of personal data, save in exceptional circumstances. Transfer within the European Economic Area is permitted. *NB* Personal data placed on the Internet will inevitably find its way outside of the EEA.

Official Secrets Acts 1911-1989

The Official Secrets Acts 1911-1989 establish severe criminal penalties for any person who discloses any material which relates to security, intelligence, defence or international relations and which has come into that person's possession through an unauthorised disclosure by a Crown Servant or Government contractor. They also cover material which has been legitimately disclosed by a Crown Servant or Government contractor on terms requiring it to

be kept confidential or in circumstances in which it might reasonably be expected to be treated as confidential. This means that certain information handled by the University's departments may be covered by the provisions of the Acts, particularly if such information concerns a project specifically commissioned by a Government office.

Defamation

Defamation consists of the publication of opinions and untrue statements which adversely affect the reputation of a person or a group of persons. If such a statement is published in a permanent form as is the case with statements published on the Internet, an action for libel may be brought against those held to be responsible.

In accordance with the provisions of the Defamation Act 1996, Coventry University is committed to taking all reasonable care to avoid the dissemination of defamatory material and it will act promptly to remove any such material which comes to its attention so far as is possible within the bounds of academic freedom. Remember that even messages which have only one intended recipient may reach a vast audience through this medium. As a result, the transmission of statements which discredit an identifiable individual or organisation may lead to substantial financial penalties.

Obscenity

Coventry University is committed to the prevention of publication of any material which it may consider pornographic, excessively violent or which comes within the provisions of the Obscene Publications Act 1959, the Protection of Children Act 1978 or the Criminal Justice Act 1988 on any of the University's computing facilities. The University will regard any such publication as a very serious matter and will not hesitate to contact the police. Users of the computing facilities are reminded that they are principally for use in connection with academic purposes or purposes related to the core business of the University. Therefore any use of the computing facilities to publish or gain access to obscene, pornographic or excessively violent material is inappropriate.

Discrimination

Current equality legislation renders unlawful discrimination on the grounds of age, race, gender, disability, sexual orientation, religion or belief. Placing or disseminating through the University's computing facilities material which may be considered discriminatory or may encourage discrimination on the above grounds is therefore likely to be unlawful and is contrary to Coventry University's Equality and Diversity Policy.

Placing discriminatory advertisements may in certain circumstances be regarded as a criminal offence under equality legislation, which establishes fines of up to £5,000 for those found guilty of causing such advertisements to be published. Inciting racial hatred by displaying any written material which is threatening, abusive or insulting is an offence under the Public Order Act 1986. Anyone found guilty of the offence of inciting racial hatred may be liable to imprisonment for up to 7 years and an unlimited fine.

Any material which constitutes harassment of an individual under the Protection from Harassment Act 1997 and the Crime and Disorder Act 1998 may also be unlawful.

Criminal Law

The incitement to commit a crime is a criminal offence in itself, regardless of whether a crime has actually been committed or not. This includes the provision of information via computerised services which facilitates any of the activities which this code has highlighted as criminal offences.

Advertisements and Commercial Activity

Vacancy advertising is provided by Human Resources. Course advertising is provided by Marketing and Communications.

Any advertising material disseminated via Coventry University's computing facilities will be subject to the JANET Acceptable Use Policy (AUP) and limited to the provision of information about courses or facilities and advertising on specific mail lists where such advertising is pertinent to the purpose of the list. This responds to the rationale followed by the AUP, which

permits uses that are socially acceptable to the community that JANET serves. In any event, the University's computing facilities must not be used for placing or distributing non-University commercial advertisements relating to any course of business.

International Law and the Internet

Since there is no international convention on Internet regulation, caution is necessary in considering what law may be applicable. As a basic rule, all users of Coventry University's computing facilities must note that although certain materials may be considered legal in their place of origin that does not prevent the application of UK law if those materials are considered to be illegal under the law in this country.

JANET Acceptable Use Policy

Background and Definitions

1. **"JANET"** is the name given both to an electronic communications network and a collection of electronic communications networking services and facilities that support the requirements of the UK education and research community. JANET is managed by JANET(UK) on behalf of the Higher Education Funding Council for England and its partner funding bodies, via their Joint Information Systems Committee (the **"JISC"**).
2. JANET is maintained primarily to support education and research within the UK public sector. It is not a public network. The *JANET Acceptable Use Policy* does not determine the eligibility of any particular organisation to have a connection to and use JANET. This eligibility is determined by the *JANET Connection Policy* which is maintained by JANET(UK) on behalf of the JISC. The JANET Acceptable Use Policy merely defines acceptable and unacceptable use of JANET by those who have been provided with a connection under the terms of the JANET Connection Policy.
3. The JANET Acceptable Use Policy is an integral part of JANET(UK)'s *Terms and Conditions for the Provision of the JANET Service* (the **"JANET Terms"**). There are a number of explanatory notes (each, a **"Note"**) at the end of this document, and referenced from individual clauses of this Acceptable Use Policy. Each Note is an integral part of the JANET Acceptable Use Policy.
4. The JANET Acceptable Use Policy applies in the first instance to any organisation authorised to use JANET (a "**User Organisation**"). It applies also to use of JANET by the User Organisation's own members and all those to whom it otherwise provides with access to JANET (collectively, its "**Members**").
5. It is therefore recommended that each User Organisation establishes its own statement of acceptable use within the context of the services provided to its Members, and in a form that is compatible with the conditions expressed in the JANET Acceptable Use Policy. Such a statement may refer to, or include, this document. If material from this document is included, this must be done in such a way as to ensure that there is no misrepresentation of the intent of the JANET Acceptable Use Policy. The JANET Service Desk can advise on this aspect as and where necessary.
6. Those implementing this JANET Acceptable Use Policy within a User Organisation should also take into account the provisions of the *JANET Security Policy* and associated guidance documents, in respect both of the connection of IT systems to JANET via the User Organisation's network and of individual Members' access to JANET.
7. Copies of the JANET Terms and of the JANET Connection and Security Policies may be found on the JANET website, via the URLS given alongside other JANET (UK) contact details at the end of this document.

Acceptable Use

8. A User Organisation and its Members may use JANET for the purpose of communicating with other User Organisations and their Members, and with organisations, individuals and services attached to networks which are reachable via JANET. All use of JANET is subject to the JANET Terms.
9. Subject to clauses 11 to 19 below, JANET may be used by a User Organisation and its Members for any lawful activity that is in furtherance of the aims and policies of the User Organisation. > **Note 1**
10. It is the responsibility of the User Organisation to ensure that its Members use JANET services in accordance with this JANET Acceptable Use Policy, and with current legislation. > **Note 2**

Unacceptable Use

11. JANET may not be used by a User Organisation or its Members for any of the activities described below. > **Note 3**

12. Creation or transmission, or causing the transmission, 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. > **Note 4**
13. Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.
14. Creation or transmission of material with the intent to defraud.
15. Creation or transmission of defamatory material.
16. Creation or transmission of material such that this infringes the copyright of another person.
17. Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to which the user or their User Organisation has chosen to subscribe.
18. Deliberate unauthorised access to networked facilities or services. >**Note 5 >Note 6**
19. Deliberate activities having, with reasonable likelihood, any of the following characteristics:
    a. wasting staff effort or networked resources, including time on end systems and the effort of staff involved in the support of those systems;
    b. corrupting or destroying other users' data;
    c. violating the privacy of other users;
    d. disrupting the work of other users;
    e. denying service to other users (for example, by deliberate or reckless overloading of access links or of switching equipment);
    f. continuing to use an item of networking software or hardware after JANET(UK) has requested that use cease because it is causing disruption to the correct functioning of JANET;
    g. other misuse of JANET or networked resources, such as the introduction of "viruses" or other harmful software via JANET.

Access to Other Networks via JANET

20. Where JANET is being used to access another network, any breach of the acceptable use policy of that network will be regarded as unacceptable use of JANET. Any deliberate activity as described in clause 19 above, and where applied to a user of that network, will also be regarded as unacceptable use of JANET.
21. Any breach of industry good practice (as represented by the standards of the London Internet Exchange) that is likely to damage the reputation of the JANET network will also be regarded *prima facie* as unacceptable use of JANET.

Passing on and Resale of JANET

22. A User Organisation may extend JANET access to other individuals on a limited basis where this is done in pursuance of the User Organisation's remit and for which it receives public funds, provided no charge is made for such access. > **Note 7**
23. It is expected that such use will be regulated by the User Organisation in the same manner as it would regulate occasional use by third parties of its other facilities, such as its telephone and IT support systems. Any individual using JANET in this manner must therefore be subject to the same requirement to use JANET in an acceptable manner as is required by the User Organisation of its Members.
24. Otherwise, a User Organisation is not permitted to provide access to JANET to third parties without the prior agreement of JANET(UK). > **Note 8**
25. This agreement will normally take the form of licensing by JANET(UK) of the User Organisation to provide such access. Details of such licensing schemes, known as *Sponsored* and *Proxy Licences*, are available from JANET(UK).

Compliance

26. It is the responsibility of the User Organisation to take reasonable steps to ensure its Members' compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of JANET is dealt with promptly and effectively should

it occur. The discharge of this responsibility includes informing all Members of the User Organisation with access to JANET of their obligations in this respect.

27. Where necessary, service may be withdrawn from the User Organisation, in accordance with the JANET Terms. Where violation of these conditions is unlawful, or results in loss or damage to JANET(UK) or JANET resources or the resources of third parties accessible via JANET, the matter may be referred for legal action.

Explanatory Notes

1. Use by the User Organisation and its members may be in pursuance of activities for commercial gain as well as for not-for-profit activities, provided such activities remain in accordance with the aims and policies of the user organisation.
2. It is preferable for misuse to be prevented by a combination of responsible attitudes to the use of JANET resources on the part of its users and appropriate disciplinary measures taken by their User Organisations.
3. The list of unacceptable activities in this section is not necessarily exhaustive. In accordance with clause 9, the use of JANET for any activity which may reasonably be regarded as unlawful is not permitted. The purpose of this section is to bring as clearly as possible to the reader's attention those activities most commonly associated with the abuse of a network.
4. It may be permissible for such material to be received, created or transmitted where this is for properly supervised and lawful purposes. This may include, for example, approved teaching or research, or the reception or transmission of such material by authorised personnel in the course of an investigation into a suspected or alleged abuse of the institution's facilities. The discretion to approve such use, and the responsibility for any such approval, rests with the User Organisation.
5. Implicit authorisation may only be presumed where a host and port have been advertised as providing a service (for example by a DNS MX record) and will be considered to have been withdrawn if a complaint from the provider of the service or resource is received either by the User Organisation or by JANET(UK). For all other services and ports, access will be presumed to be unauthorised unless explicit authority can be demonstrated.
6. Where a User Organisation wishes to commission or itself perform a test for vulnerabilities in its IT systems (for example, via "penetration testing") this, as an action authorised by the User Organisation, will not be a breach of clause 18. However, the User Organisation should inform the JANET CSIRT, in advance of the test, of the source, nature and timing of the test. This is to avoid wasting the time and resources of the CSIRT in investigating the perceived attack on the User Organisation, or automatically blocking it
7. It is intended that this provision be used, for example, to permit a guest of the User Organisation to gain access to JANET for the purpose of maintaining contact with his or her home organisation, or of carrying out his or her teaching or research activities whilst using the User Organisation's facilities. It is expected that such use will be occasional and reasonably time-limited.
8. A third party, where an individual, means someone who is not acting as a Member of the User Organisation. Where it applies to a separate organisation, this is defined to be any organisation that is in law a separate entity to the User Organisation.

JANET(UK) Contact Details and URLs

JANET Service Desk:
Email: service@ja.net
Tel: 0870 850 2212

JANET CSIRT:
Email: irt@csirt.ja.net
Tel: 0870 850 2340

JANET Terms: www.ja.net/services/publications/policy-documents/terms-for-theprovision-of-the-janet-service

JANET Policies: www.ja.net/services/publications/supportmanual/policies