

ACCEPTABLE USE POLICY REGARDING THE UTILISATION OF COLLEGE IT RESOURCES AND ACCESS TO COLLEGE ADMINISTRATIVE SYSTEMS, USE OF THE INTERNET AND EMAIL

1 SCOPE

- 1.1 The College's Internet access is provided by the United Kingdom Education & Research Networking Association (UKERNA). UKERNA have developed and now operate The Joint Academic Network (JANET) under a Service Level Agreement from the Joint Information Systems Committee (JISC) of the UK Higher and Further Education Funding Councils.
- 1.2 UKERNA requires the College to agree to abide by and adhere to various terms and conditions when using the service. The most important obligations placed on College staff and students using the JANET system are as follows:

"The User Organisation (the College) will ensure that all use of JANET by its members, staff, students and anyone else to whom JANET is made available by the User Organisation conforms to the current versions of the JANET Acceptable Use Policy and its Security Policy."
- 1.3 Failure to comply with these Terms and Conditions may lead to the loss of the service, i.e., the link to the Internet. It is essential that all users of Internet and Internet email are made aware of the contents of these policies and adhere to them.
- 1.4 JISC & UKERNA also recommend that every HE & FE College instigates its own Acceptable Use of IT Policy (AUP) to make all users aware of the Terms and Conditions laid down by UKERNA as to the AUP of JANET and to protect itself and its staff by making them aware of all relevant legislation.
- 1.5 This code applies to all users of College computer facilities, i.e., all staff (academic and support) and all students.

2 AIMS

- 2.1 To ensure security and proper use of College IT Systems.
- 2.2 To safeguard The College's business operations.
- 2.3 To inform all users (staff and students) of all relevant legislation relating to IT.
- 2.4 To provide an appropriate teaching and learning environment for all College IT Users.
- 2.5 To ensure all users of College IT Systems are aware of the Terms and Conditions laid down by UKERNA.

3 INTERNET AND INTERNET EMAIL USAGE

- 3.1 Use of the Internet for College work purposes is encouraged and permitted within the following guidelines:
 - It complies with the JANET AUP
 - It does not contravene any applicable legislation.
- 3.2 Reasonable private and personal use of the Internet is encouraged and permitted for College staff within the guidelines as in 3.1 above and it is carried out in the user's own time. Private internet use must not interfere with or take priority over College work. This access is provided free of charge to College employees.
- 3.3 The College undertakes to provide an internet email account for all staff and students as "[username](mailto:username@bpc.ac.uk)@bpc.ac.uk
- 3.4 Only College email addresses may be used on College publications.
- 3.5 College email addresses may not be used other than on College websites.
- 3.6 There may be certain periods when private use of the internet will not be permitted, for example during enrolment and on-line examinations.
- 3.7 Copyright applies to all text, pictures, video and sound, including those sent by e-mail or on the Internet. Files containing such copyright protected material may be downloaded, but not forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate. Please note that all copyright in emails, prepared by staff in the course of their work belongs to the College.
- 3.8 Copyrighted software must not be downloaded. Such copyrighted software will include screen-savers. *See College Control Procedure 4.6*
- 3.9 Copyrighted music, video and sound may not be downloaded.
- 3.10 All computer software should be purchased through MITS to ensure that the College is compliant with licensing agreements.
- 3.11 Users should not import non-text files or unknown messages on to The College's system without having them scanned for viruses. College systems automatically scan for known viruses. If a virus is detected, contact MITS immediately.

- 3.12 All users must abide by the College's procedure on email usage [link]
- 3.13 All College web pages must conform to the SENDA guidelines.
- 3.14 Staff must notify LSS where any IT equipment does not meet the SENDA guidelines.

4 MONITORING AND INTERCEPTION OF DATA

- 4.1 The College reserves the right to monitor usage of all College IT facilities in order to:
- ensure the security of its systems
 - to safeguard those systems from virus infection and spam invasion
 - to monitor and prevent access to inappropriate internet sites in order to provide as secure an environment for students as possible. *For further information, see Appendix 3*
 - to ensure compliance with the JANET AUP and Security Policy
- 4.2 In order to comply with current legislation, [*Regulation of Investigatory Powers Act 2000, the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations and Data Protection Code of Practise*], it is necessary for The College to obtain the express permission of all users to enable the monitoring of these systems. College staff will supply their express permission by signing the user application form. Students will give their consent by connecting online to validate their network login.

5 GENERAL USAGE

- 5.1 College staff and students are responsible for safeguarding their password(s) for the system(s). For security reasons, individual password(s) must not be printed, stored on-line or given to others.
- 5.2 A User's ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so.
- 5.3 Advertising - Users of College IT resources are not permitted to create, place or distribute any advertisement which is of a commercial nature.
- 5.4 Staff may use the College Voice systems for personal use providing they notify the College switchboard prior to the commencement of the personal call, and at its cessation, to enable user billing. The College operates a call logging system that monitors the duration, source and destination of all incoming and outgoing calls.
- 5.5 The Internet is not a secure medium and other Internet users may be able to obtain information regarding your activities while you use the Internet. The College accepts no responsibility for any loss, financial or otherwise, resulting from the use of Internet services by any party. If you choose to transmit confidential information such as address, credit card or financial details it is your responsibility to assess the risk of this information being available to other parties.

Signed: (Rowland Foote) **Date:** October 2006

Designation: Principal of Bournemouth and Poole College

Policy ref./version number: CO5/V6

This Policy is to be reviewed by the College Information Technology Group by: October 2009.

Appendix 1

LEGAL FRAMEWORK

JANET Acceptable Use Policy

The Joint Academic Network (JANET) is a facility to which The Bournemouth & Poole College subscribes and which supports the communication requirements of the United Kingdom education and research community. In subscribing to such facilities, The Bournemouth & Poole College undertakes to adhere to the JANET Acceptable Use Policy. All Internet traffic is routed via The College's JANET connection and The College requires that all users of College computer resources are aware of and comply with the requirements of the Acceptable Use Policy. See Appendix 2 or visit [<http://www.ja.net/documents/use.html>].

Statutory and other provisions of English Law

Whilst the use of the Internet is a broadly unregulated medium, there are a number of statutory and other legal provisions which may impact upon its use. The following are a selection of provisions for which users of the Internet will need to be cognisant; they are, however, by no means exhaustive. It must also be noted that it is the policy of The Bournemouth & Poole College to refer to the appropriate authorities any discovery of a breach of the law arising from use of the Internet.

1 *Computer Misuse Act 1990*

The Computer Misuse Act 1990 makes it a criminal offence to access, or attempt to access, computer material without proper authority or to make unauthorised modification of computer material. Persons convicted of an offence under the Computer Misuse Act are subject to a maximum of 5 years' imprisonment or a fine or both. In the context of Internet use, it is likely that the following examples would be considered illegal:

- Accessing restricted material without proper authority.
- Provision of any material, such as codes or 'hacking' instructions which enables others to gain unauthorised access to a computer system.
- Knowingly receiving (or using) any material from an unauthorised user who has gained access to systems.
- Unauthorised modification of a computer system program or data stored on a system.
- Any material which encourages or incites other persons to carry out unauthorised access or modification of a computer system, program or data.

2 *The Copyright Designs and Patents Act 1988*

It is an offence under this Act to copy software or other Internet materials without authority (see paragraphs 7.1.1 and 7.8 of College Copyright Control Procedure 3.17). It is immaterial whether such unauthorised copying is done with a view to personal convenience or for monetary gain. Unlimited fines and up to two years' imprisonment may be imposed on offenders.

All software, including commercial products and Shareware, is protected by copyright law and is licensed for legitimate use. Some software creators have designated their products Freeware (for which use is authorised without a licence fee being payable) and have made this available on the Internet. The College does not tolerate the use of unauthorised/unlicensed software and may require evidence from any user of software obtained via the Internet that its use is lawful.

3 *Data Protection Act 1984*

This Act prohibits the holding, processing or disclosure of personal information data about others on computer, unless the data user is properly registered and observes the data protection principles. In view of the complexity of the legislation, all students of The Bournemouth & Poole College are prohibited from establishing, holding or processing any personal data concerning other persons on any College computer and this includes both 'uploading and downloading' of such data via the Internet.

Staff use is subject to The College's Data Protection Registration and it is the duty of each staff user of College computer facilities to ensure that their use complies with the Data Protection Act and is within The College's Registration. The Data Protection Principles and the details of the other provisions of the Act and The College's Registration may be obtained from The College's Data Protection Officer. Additional information [http://www.jisc.ac.uk/legal/data_protection.html] and [<http://www.dataprotection.com>]

4 *Race Relations and Sexual Discrimination Acts*

Discrimination on the grounds of race, colour, nationality, ethnic or national origin or gender is unlawful under the provisions of the above legislation. Any material published or received via the Internet (or by other means) which discriminates or encourages discrimination is in contravention of the legislation.

5 *Regulation of Investigatory Powers Act (RIPA) 2000*

RIPA prohibits the interception of e-mails without first obtaining the consent of both the sender and the recipient. However, the Regulations, which came into force on 2 October 2000, provide an important exception to the general rule that communications may only be monitored with consent.

The regulations enable businesses to intercept telecommunications without the consent of their employees for certain legitimate purposes, including detecting unauthorised use of the system and ensuring its efficient operation. However, the employer must make reasonable efforts to inform employees that communications may be monitored. Additional information : [<http://www.jisc.ac.uk/legal/encryption.html>]

6 *The Human Rights Act 1998*

Article 8 of the Human Rights Act states that "everyone shall have the right to respect for his private and family life, his home and his correspondence". However, this right is qualified and may be interfered with in order to protect the rights and freedoms of others. An employer, for example, may claim that, by monitoring e-mails, it is protecting the rights of other employees to have a

workplace which is free of discrimination (assuming the employer prohibits the sending of discriminatory material via e-mail). Similarly, the employer may legitimately argue that, by having CCTV, it is providing its employees with a safe work environment and further, taking action which is necessary to prevent crime. Additional information: [http://www.jisc.ac.uk/legal/human_rights.html]

7 *Official Secrets Act*

The provisions of this legislation often apply in connection with contracts with the Government or Government agencies. Any publication of material via the Internet (or by other means) which is in contravention of obligations under the Official Secrets Act is a criminal offence which is punishable by imprisonment or a fine or both.

8 *Criminal Justice and Public Order Act 1994*

This miscellany of legislation includes a consolidation of provisions for the protection of minors by making it a criminal offence to possess pornographic or obscene material of or involving minors, or material considered to be excessively violent. In the context of the Internet it would apply to the transmission, receipt and storage of text, audio and graphic images.

9 *Laws of Defamation*

Any publication of a statement, comment or innuendo about another individual or organisation which cannot be justified at law may render the author liable to an action of defamation. In the context of Internet use, The College will not permit the publication of defamatory material and any author transmitting or any person passing on defamatory material will be required to indemnify The College against all actions, proceedings, claims and costs resulting therefrom.

10 *Obscene Publications Act 1959*

The publication (whether for gain or not) of material intended to be read, heard or looked at which is as to tend to deprave and corrupt persons having access to the publication is a criminal offence which carries a maximum sentence of three years' imprisonment.

11 *Telecommunications Act 1984*

A person who sends a message or other matter that is grossly offensive, indecent, obscene or menacing in character via the public telecommunication system or sends a false message for the purpose of causing annoyance, inconvenience or needless anxiety to another shall be guilty of a criminal offence. The Internet makes use of the "public telecommunication system". A breach of this Act will result in a substantial fine and/or imprisonment.

12 *The Special Needs and Disability Act 2001 (SENDA)*

This Act places a requirement on those responsible for the provision of education not to discriminate against disabled students in the supply of educational services. Both institutions and individuals have a responsibility under the legislation not to discriminate against disabled students by giving less favourable treatment (including victimisation) or by failure to make reasonable adjustments. For further help and advice contact LSS.

International Law

Users of the Internet should be aware that any material which they create and transmit is accessible world-wide and that such material must not therefore contravene any international laws or treaties. Specific examples include the possibilities that material lawfully provided in the United Kingdom but accessed in another country may constitute an offence within that recipient country.

Appendix 2

JANET Acceptable Use Policy

Version: 7.0

Date: July 2003

Editor: Shirley Wood

Contents

- Background and Definitions
- Acceptable Use
- Unacceptable Use
- Passing on and Resale of JANET Service
- Compliance

Background and Definitions

1. "JANET" is the name both to an electronic communications network and a collection of electronic communications networking services and facilities that support the requirements of the UK higher and further education and research community. JANET is managed by UKERNA on behalf of the Joint Information Systems Committee (JISC) and is not for public use.
2. The Higher Education Funding Councils for England, Scotland and Wales, the Learning and Skills Council, the Scottish Further Education Funding Council, the National Council for Education and Training for Wales and the Department of Higher and Further Education, Training and Employment are responsible jointly for the provision of JANET. They exercise this responsibility through their Joint Information Systems Committee (the JISC) and any dispute over the interpretation of this Policy will be resolved by the JISC.
3. UKERNA (an acronym for the United Kingdom Education and Research Networking Association) is the trading name of the company contracted by the JISC, acting in the name of the Higher Education Funding Council for England, for the provision of the JANET service. This includes the day-to-day management of this Policy.
4. This Policy applies in the first instance to any organisation authorised to use JANET (a "User Organisation"). It is the responsibility of User Organisations to ensure that members of their own user communities use JANET services in an acceptable manner and in accordance with current legislation.
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 users, and in a form that is compatible with the conditions expressed in this 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 this Policy. UKERNA can advise on this aspect as and where necessary.
6. JANET is maintained to support teaching, learning and research. The connection of any organisation to JANET is governed by the JANET Connection Policy maintained by the JISC. JANET is not a public working network.

Acceptable Use

7. A User Organisation may use JANET for the purpose of interworking with other User Organisations, and with organisations attached to networks which are reachable via interworking agreements operated by UKERNA. All use of JANET is subject to payment of the appropriate charges in force during the period of service. Any provision of service must be authorised in advance.
8. Subject to the following paragraphs, JANET may be used for any legal activity that is in furtherance of the aims and policies of the User Organisation.

Unacceptable Use

JANET may not be used for any of the following:

- 9.1 the creation or transmission (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;
- 9.2 the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;
- 9.3 the creation or transmission of defamatory material;
- 9.4 the transmission of material such that this infringes the copyright of another person;
- 9.5 the transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks, save where that material is embedded within, or is otherwise part of, a service to which the member of the User Organisation has chosen to subscribe;
- 9.6 deliberate unauthorised access to facilities or services accessible via JANET;
- 9.7 deliberate activities with any of the following characteristics:
 - wasting staff effort or networked resources, including time on end systems accessible via JANET and the effort of staff involved in the support of those systems;
 - corrupting or destroying other users' data;
 - violating the privacy of other users;
 - disrupting the work of other users;
 - using JANET in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of switching equipment);
 - continuing to use an item of networking software or hardware after UKERNA has requested that use cease because it is causing disruption to the correct functioning of JANET;
 - other misuse of JANET or networked resources, such as the introduction of "viruses".
10. Where JANET is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of JANET. Any breach of industry good practice (as represented by the standards of the London Internet Exchange), or of the Acceptable Use Policies of other networks, that is likely to damage the reputation of the JANET network may be regarded as a breach of this AUP.

Passing on and Resale of JANET Service

11. It is not permitted to provide access to JANET for third parties without the prior agreement of UKERNA, with the exceptions in the following sub-paragraphs.
 - 11.1 The JISC has resale schemes whereby certain types of User Organisation may sell on JANET services under defined circumstances. Details may be obtained from UKERNA.
 - 11.2 It is acceptable for a User Organisation connected to JANET to extend access to others on a limited basis, provided no charge is made for such access. For example, it is acceptable that a visitor to the Organisation be permitted to gain access to JANET for the purpose of maintaining contact with his or her home organisation. It is intended that such use 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.
12. 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.

Compliance

13. It is the responsibility of the User Organisation to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of JANET does not occur. The discharge of this responsibility must include informing those at the Organisation with access to JANET of their obligations in this respect.
14. Where necessary, service may be withdrawn from the User Organisation. This may take one of two forms.
 - 14.1 An indefinite withdrawal of service, should a violation of these conditions persist after appropriate warnings have been given by UKERNA. Such a withdrawal of service would only be made on the authority of the JISC. Restoration would be made only when the JISC was satisfied that the appropriate steps had been taken at the Organisation involved to ensure acceptable behaviour in future.
 - 14.2 A suspension of service, should a violation of these conditions cause serious degradation of the service to other users of JANET. Such a suspension would be made on the judgement of UKERNA, and service would be restored when the cause of the degradation of service to others had been removed.
15. Where violation of these conditions is illegal or unlawful, or results in loss or damage to UKERNA or JANET resources or the resources of third parties accessible via JANET, the matter may be referred for legal action.
16. It is preferable for misuse to be prevented by a combination of responsible attitudes to the use of JANET resources on the part of users and appropriate disciplinary measures taken by their Organisations.

Trademarks:

"JANET" and "UKERNA" are trade marks of the Higher Education Funding Councils for England, Scotland and Wales, which have granted the JNT Association the right to use the marks.

Disclaimer:

Neither the Higher Education Funding Council for England nor the JNT Association can accept any liability for any loss or damage resulting from the use of the material contained herein. The information is believed to be correct but no liability can be accepted for any inaccuracies.

Availability:

Further copies of this document may be obtained from the JANET Customer Service, UKERNA, Atlas Centre, Chilton, Didcot, Oxfordshire, OX11 0QS.

Copyright The Higher Education Funding Council for England, 1995 - 2003

Appendix 2a 6 JANET Security Policy

September 1995
© 2005 Joint Information Systems Committee

Background

1. It is the policy of the JISC that, as a network for education and research, JANET will be most effective if it places as few technical restrictions as possible on the development or use of new applications and services. The imposition of mandatory access control or monitoring systems is likely to cause problems for existing uses of the network as well as limiting future developments, and should only be considered where there is a clear benefit. Filtered or restricted network access may be offered as optional services that organisations can join, however the core JANET service should provide as open a network as is possible while meeting operational and legal requirements.
2. A presumption of openness brings associated risks that security incidents or misuse will seriously damage the effectiveness of the network (a summary of these risks can be found in Annex A). The impact of incidents may rapidly spread far beyond the individual organisation, machine or user where they originate. These risks must be managed if the network is to fulfil its purpose. The JISC has therefore adopted this Security Policy to protect the network and the organisations that use it. Under the Terms for the Provision of the JANET Service, compliance with this Policy is a requirement for all organisations connected to the network. The Policy also places responsibilities on users of the network. The authority of UKERNA, as service provider, to protect the operation of the network is established in the Terms for the Provision of the JANET Service.
3. This JANET Security Policy therefore has a number of goals:
 - To ensure that appropriate local policies exist to protect JANET, the networks connected to JANET and the computer systems using JANET from abuse (whether defined in this or other JANET Policies);
 - To ensure that mechanisms exist to aid the prevention and identification of abuse of the JANET network;
 - To ensure an effective response to complaints and queries about real or perceived abuses of the JANET network;
 - To ensure that the reputation of JANET is protected and that the network can meet its legal and ethical responsibilities with regard to its connectivity to the worldwide Internet.

Definitions

4. The term 'User Organisation' has the meaning defined in the Terms for the Provision of the JANET Service.
5. The term 'Connected Organisation' means any organisation with a connection to the JANET network, whatever type of licence covers the connection. In particular it includes User Organisations.

The Policy

Responsibilities

6. The Terms for the Provision of the JANET Service place responsibilities on every person and organisation involved in the use or operation of JANET to protect the network against security breaches. In particular:
 - Each User Organisation must ensure that all use of JANET by those individuals and Connected Organisations to whom it provides network access complies with this Security Policy and the JANET Acceptable Use Policy. The User Organisation must also ensure that information about security issues can be communicated rapidly within the organisation and to UKERNA and that problems are resolved promptly (see paragraphs 7 and 8);
 - Each Connected Organisation, including those that are User Organisations, must ensure that its actions and those of the users for which it is responsible are safe for themselves and do not present a threat to others (see paragraph 9);
 - Each user of the JANET network and the networks of Connected Organisations must behave in accordance with this Security Policy and with any policies and procedures local to the Connected Organisation. The user must cooperate with their organisation and the network operators to reduce security risks;
 - UKERNA must ensure that the operation of the network is appropriately monitored, that the response to security problems is coordinated, and that temporary or permanent measures are implemented, up to and including disconnection, where necessary to protect the network or to comply with the law (see paragraph 10).

Points of Contact at the User Organisation

7. The successful prevention of security incidents and prompt resolution of those that do occur both depend critically on the rapid and accurate transfer of information between JANET Connected Organisations and UKERNA as operator of the network. To this end each User Organisation must provide UKERNA with up-to-date details of one or more persons who will act as Security Contact(s) for the User Organisation and any other organisations and individuals to whom the User Organisation provides access to JANET. The User Organisation must ensure that its designated Security Contact(s) have appropriate knowledge, skills, resources and authority to fulfil their role (see note 1).
8. The Security Contact(s) have roles in both the prevention and resolution of security incidents:
 - To disseminate UKERNA's warnings of general risks and precautions to appropriate people within the organisation(s) for which they are responsible, and to ensure that appropriate preventive measures are taken promptly;
 - To ensure that any particular security breach or risk that has been reported to the Security Contact(s) by UKERNA as affecting an organisation for which they are responsible is investigated and resolved promptly, and to inform UKERNA that this has been done.

Responsible Action by the Connected Organisation

9. Each Connected Organisation must act responsibly to protect the network. This duty includes:
 - Taking effective measures to ensure that there is no security threat to JANET or other Connected Organisations from insecure devices connected to the Organisation's network (see note 2);
 - Taking effective measures to protect against security breaches, in particular ensuring that recommended security measures are implemented;
 - Taking effective measures to ensure that security breaches can be investigated and that other users of the network are protected from the consequences of breaches;
 - Assisting in the investigation and repair of any breach of security;

- Promoting local policies in support of this JANET Security Policy, backed by adequate disciplinary and other procedures for enforcement;
- Implementing appropriate measures for giving, controlling and accounting for access to JANET, backed by regular assessments of the risks associated with the measures chosen (see note 3);
- Taking reasonable measures to encourage its users to act responsibly in compliance with this Policy and the JANET AUP, and ensuring that they are enabled to do so through systems, procedures and training that support good security practice.

Monitoring and Enforcement by UKERNA

10. The Terms for the Provision of the JANET Service authorise UKERNA, as the service provider responsible for the JANET network, to require connected organisations to comply with this Policy, to monitor the network where it has reason to believe there has been a breach of the Policy or other threat, and to take such actions as are necessary to protect the operation of the network and the security of services provided to JANET customers (see note 4). In particular UKERNA is authorised to:
 - Monitor use of the network, while respecting privacy and national law, either in response to information about a specific threat or generally because of the perceived situation;
 - Implement such temporary technical measures as are required to protect the network or its customers against breaches of security or other incidents that may damage the network's service or reputation;
 - Require a User Organisation, through its nominated contact, to fulfil its responsibilities under any of the JANET Policies;
 - Where a User Organisation is unable or unwilling to co-operate, initiate the process for achieving an emergency disconnection;
 - Where permitted or required by law, assist law enforcement authorities in their investigations concerning the JANET network.

Explanatory Notes

1. Further details of the role of the Security Contact can be found in the JANET Support Handbook on the JANET website.
2. The security of networked devices may, for example, be managed by a combination of direct configuration and maintenance, technical controls such as firewalls or router access control lists, system monitoring or probing, and delegation to appropriately skilled others. Where an organisation allows a device it does not own or control to connect to the network it is strongly recommended that consent to these normal operational measures be obtained as a condition of connection.
3. Further information about granting and accounting for access can be found in the factsheet 'User Authentication' on the JANET website.
4. On occasion, Regional Network Operators may assist in the investigation of misuse or protection of the network under their contracts with UKERNA.

Annex: Risks to Networks and Networked Systems

All computer networks are exposed to threats, both internally and from the other networks to which they connect. Hostile traffic, both random and directed, is now a constant feature of the Internet. The particular open character of an education and research network increases both its exposure to these threats and the potential damage to the integrity and effectiveness of the network.

The risks to the network, the computers and organisations connected to it, include:

- Breaches of confidentiality. Organisations hold and have access to large amounts of intellectual property, both their own and licensed from others: the value of such property may be greatly reduced if it is disclosed to others. Organisations also handle a great deal of personal information about individuals who may suffer if it is not kept confidential: consequences range from a loss of privacy to partial or complete theft of identity.
- Loss of integrity. Information held on computers can be destroyed or modified, and unauthorised changes may be undetectable. The integrity of computers themselves may be compromised if intruders are able to take control of them, thus casting doubt on the accuracy of any results and the privacy of any data. Repeated failures can result in users losing confidence in computer systems at their own or other organisations.
- Failures of availability. Networks and the computers connected to them may be temporarily disabled either deliberately or accidentally by large flows of network traffic, making them unusable at critical times. Organisations that lose the confidence of others may find themselves unable to communicate if they are placed in a blacklist. Network and computer staff may be unavailable for support or development activities if they have to spend their time dealing with security incidents.
- Damage to reputation. The reputations of JANET and the organisations and individuals connected to it may be seriously harmed by security incidents or inappropriate use of the network. Many intruders like to advertise their successes, others may attack third parties using computers connected to JANET and to which they have gained control. Organisations whose systems are used in these ways are likely to be held responsible. The use of JANET to disseminate unwanted, offensive or illegal material is also likely to be seen as misuse of a publicly-funded resource.
- Legal action. National and international law is increasingly concerned with data networks and is placing a growing list of obligations on those who provide them. Individuals, organisations and network operators who, by action or inaction, fail to meet their legal obligations may be punished by the criminal law, have substantial financial damages awarded against them or be required to modify or cease their networking operations.

The openness of JANET and other connected networks may allow the impact of a security breach to spread far beyond an original insecure system or action. The same openness means that it will rarely be possible to protect organisations and users against the immediate consequences of their insecure actions: more often it will be necessary to respond promptly to security breaches by isolating the systems and organisations affected until the problem has been resolved.

Appendix 3

Guidelines for using the Internet and Internet email

1 The Internet

- All use of the Internet can be tracked and users should be aware that all sites accessed are automatically recorded in a file in their personal profile. The reason for this is not to monitor site access, but to improve performance by speeding up access to regularly used sites. However a side effect of this means that tracking **can** be carried out.
- Additionally, many Internet sites record visitors details care should be taken when disclosing personal and finance details.
- Training and information sessions on the use of the Internet are available. Contact Staff Development for more information.
- The College uses a system which automatically bans known inappropriate, obscene or pornographic sites. However, these are constantly changing and if any user accidentally accesses any site which is inappropriate, make a note of the address of the site (found in the location box near the top of the screen) and then contact MITS and the site can then be banned manually. For more information about The College policies regarding firewalling and security, refer to the College Computer Security Reports and The College ILT Strategy.

2 Internet Email

- Users should keep their passwords secret. If going on leave or away from work for any reason, arrange to proxy your email to another member of staff – do not pass your password onto anyone else.
- Emails and attachments may be scanned to detect viruses, oversize or obscene items.
- Manual email content monitoring and interception would only be carried out in the event of technical problems, i.e. virus infection or file corruption or on behalf of or by the police as part of a criminal investigation [see Appendix 1]. Automatic scanning of emails and attachments may be set to check for executables, certain types of graphics, attachments over a certain size, etc.
- Users should be aware that, in law, emails are regarded as equivalent to written correspondence. It is therefore important to take care not to express yourself in emails in any way that could be regarded as defamatory.
- Internet email is not secure - do not send confidential or sensitive data by this method.

3 Examples of Unacceptable Use

- Engaging in computer games on the Internet.
- Engaging in "chain mail".
- Inappropriate use of chat rooms for non-educational purposes.
- Transmission or receipt of large files (in particular graphic files) that may prove detrimental to College systems and other users of those systems.
- Transmission or receipt of abusive or offensive images.
- Downloading files or programs without following College procedures (i.e. to ensure system compatibility, virus checking, licensing and copyright compliance). If in doubt, contact MITS for advice and assistance.
- Engaging in gambling on the Internet.

4 Useful Links

The following sites provide further information about the use of IT and the Internet and legal implications.

- <http://www.tuc.org.uk/law>
- <http://www.out-law.com>
- <http://www.ja.net>
- <http://surfcontrol.com>
- <http://www.jisc.ac.uk>
- <http://www.dataprotection.com>