Southern Regional College

NETWORK ACCEPTABLE USE POLICY

Process Area	**ICT**
Reference Number	**ICT/001**
Author	**S Todd**
Approved by	**SMT**

Issue No	Date	Details	Author	Approved
001	Feb 2008	First Issue	ICT MG	SMT
002	Jan 2013	Updates to all sections	S Todd	SMT

If requested, the College will make the policy available by means of alternative formats including large print, Braille, audio cassette and computer disc. The policy can also be downloaded from the College intranet and made available in alternative languages as required.

1. POLICY STATEMENT

Southern Regional College will provide access to a range of information resources to assist teaching and learning, research and information handling. In addition, teaching and support staff will have restricted access to a range of business support applications through NICIS. This represents a considerable commitment of College resources in the areas of telecommunications, networking, software, storage and cost.

The Network Acceptable Use Policy is designed to outline for staff, learners and other authorised users the conditions of use for these resources.

1.1 Commitment

The College is committed to providing an effective and responsive network for use by staff and learners. Whilst the College will continue to invest in the network infrastructure there is a clear need to outline the issues that affect all staff, learners and other authorised users using the network and Internet.

1.2 Issues

Productivity – the information and resources available through the College's network can help staff, learners and other authorised users to be more productive and effective in their teaching and learning. If the Internet is subject to misuse however, it can have a significant negative effect on performance.

Bandwidth management – video, music, sound and on-line images are data intensive and can be a considerable drain on valuable network bandwidth. Similarly, heavily accessed sites that are not relevant to staff, learners and other authorised users bring unnecessary increase in network traffic.

Legal liability – Any network user who visits illegal or offensive web sites and downloads material may commit a criminal offence. Furthermore, if staff, learners and other authorised users casually visit a site which a college sees and finds offensive, the College could be held liable for not taking steps to prevent such material from being displayed.

Adverse publicity – Several companies have been forced to dismiss employees that were found guilty of accessing illegal and offensive material through the Internet. Adverse publicity relating to staff, learners and other authorised uses can clearly be very damaging.

Security- Network users can use the Internet to send and receive information that could be infected with viruses. Such viruses if allowed could infect the entire network system.

The College is committed to implementing a series of measures to ensure that the risk to its network system is minimised and that users are made aware of what is deemed acceptable use of network resources.

2. SCOPE

This policy refers to

- All users of the colleges ICT facilities.

3. DEFINITIONS

ICT	Information Communication Technology
JANET	Joint Academic Network, the college's internet service provider
Social Networking Sites	Includes but is not limited to: e-mail, blogs, forums, micro-blogging, social networking, social network aggregation, wikis, social bookmarking and tagging, photo sharing, video sharing, and virtual worlds. It is acknowledged that the scope of this policy will continue to evolve as new technologies and tools become available.
Hacking	Intentionally interfere with the normal operation of the network, including the propagation of computer viruses, by-passing filtering systems or sustained high volume network traffic which substantially hinders others in their use of the network.

4. PROCEDURE FOR IMPLEMENTATION

4.1 Strategy

It is recognised that there is no present or future technical solution which can completely guarantee the restriction of staff, learners and other authorised users to unwanted Internet material or inappropriate use. However, the following measures will be implemented:

Statement of Compliance - Use of network and Internet resources, by staff, learners and other authorised users, is encouraged but will only be permitted upon acceptance of the College's Acceptable Use Policy. All users will be expected to accept the Policy and staff will sign a statement of compliance.

Instruction - All staff, learners and other authorised users will require a level of instruction in accessing the Internet and using the College's network. Learners will receive instruction from their tutors directly during the learner induction period. Teaching and support staff are regularly instructed in the use of network applications through the College's Employee Development programme.

Joint Academic Network (JANET) – All users are expected to adhere to the conditions of use set out in the JANET Acceptable Use Policy. For details please refer to www.ja.net

4.2 General Principles

College provided Internet/Intranet and e-mail privileges, like computer systems and networks are considered College resources and are intended to be used for business and/or educational purposes related to the College. It is acknowledged that staff may occasionally use e-mail and browse the web for personal use, however, this should only be undertaken in the employees own time and is subject to the same conditions of use as stated below. No other personal use of College network resources is permitted.

Internet use and correspondence via e-mail is not guaranteed to be private. Use of Internet/Intranet and e-mail may be subject to monitoring for security and/or network management reasons. Confidential e-mails should not be sent without encryption. Users may also be subject to limitations on their use of such resources as outlined below.

Files stored on the College's network should only be stored for business use and as such are deemed accessible by the Chief Executive or delegated authority.

All existing College policies and regulations apply to a user's conduct on the Internet and Network, especially (but not exclusively) those that deal with unacceptable behaviour, privacy, misuse of College resources, harassment, information and data security and confidentiality.

The distribution of any information through the Internet, computer based services, e-mail and messaging systems is subject to scrutiny of the Chief Executive. The Chief Executive or delegated authority reserves the right to determine the suitability of this information.

4.3 Monitoring

The College respects the privacy and academic freedom of staff and students. However, the College may carry out lawful monitoring of IT systems. Staff, students and any other authorised users should be aware that the College may access email, telephone and any other electronic communications, whether stored or in transit. This is in order to comply with the law and applicable regulations and to ensure appropriate use of the College IT systems. All access and monitoring will comply with UK legislation including the Human Rights Act 1998 (HRA) and the Data Protection Act 1998 (DPA).

The College's technical support function, in the course of normal business, may access communications for a number of purposes including but not limited to the following:

- to ensure the operational effectiveness of the service. (for example, the College may take measures to protect the telecommunications system from viruses and other threats such as hacking or denial of service attacks);

- to prevent and detect crime (including, but not limited to, crimes such as fraud and unauthorised access to a computer system under the Computer Misuse Act 1990);

- to establish the existence of facts relevant to the business of the institution (for example, - where a case of suspected plagiarism is being investigated and there is sufficient evidence, the contents of an individual's communications and/or files may be examined without their consent and with the authority of an authorised person. Another example may be checking email accounts when staff are absent on holiday or on sick leave to access relevant communications);

- to investigate or detect unauthorised use of the systems (for instance, to check whether the user is breaking regulations);

- to ascertain compliance with regulatory or self-regulatory practices or procedures relevant to the College's business (i.e. to ascertain whether the College is abiding by its own policies);

- to ascertain or demonstrate standards which are achieved or ought to be achieved by persons using the system (for instance, staff training or quality control, but not for market research);

- to monitor whether or not communications are relevant to the business of the College (for example, to check an email account to ensure that it is not being used for

personal or private purposes but not to look at the contents of the emails unless this is required to confirm the use of the email account);

The College will monitor and record all Internet usage, chat, newsgroup and e-mail messages. The College reserves the right to do this at any time. No user should have any expectation of privacy as to his or her Internet usage.

4.4 Conditions of use

Users shall not:

- Create, transmit, visit or search for Internet sites that contain obscene, hateful or other objectionable materials; send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person;
- Use the Internet or e-mail for any illegal purpose;
- Represent personal opinions as those of the College;
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the College;
- Download any software or electronic files without implementing virus protection measures that have been approved by the College;
- Hack in any form;
- Reveal or publicise confidential or proprietary information which includes, but is not limited to: financial information, new business ideas, strategies and plans, databases and the information contained therein, computer network access codes and technical information;
- Examine, change, or use another person's files, output or user name for which they do not have explicit authorisation;
- Use other network facilities for personal use unrelated to College business e.g. personal email and web browsing. Network storage areas and removable media will be viewed as College property. The Network Manager or his nominee may review files and communication to ensure that users are using the system responsibly. Users are therefore asked to ensure that materials used on the College's network are for educational or College use only;
- Install software with out the expressed permission of ICT Support;
- Connect any networkable device to the College's networks without the approval of ICT Support.
- Perform any other inappropriate uses.

4.5 Social Networking Sites (Chats, Discussion forums and Newsgroups etc)

Please refer to the College Social Media Policy.

4.6 Passwords and User Ids

Any user who registers on the College network and obtains a password and ID must keep that password confidential.

User Ids and passwords will help maintain individual accountability for Internet resource usage.

The sharing of User Ids and passwords is prohibited.

It is the responsibility of all network users to change their passwords regularly.

4.7 Use of LRC and any Open Access Facilities

Staff, learners and other authorised uses wishing to use open access IT facilities must be registered users of the network.

Learners using the Learning Resource Centre must use these facilities for work associated with their course of study. Facilities should not be used for personal entertainment or use.

Staff using IT facilities must only use such resources for College related purposes.

Open access IT facilities are solely for use by staff, learners and other authorised uses of Southern Regional College. Consequently, you may be asked to show evidence of registration by producing a student card. Failure to produce a student card may lead to expulsion from the workshop or library.

4.8 Summary

Users who violate any of the conditions set out in this policy will be subject to the appropriate disciplinary procedures. The College also retains the right to report any illegal violations to the appropriate authorities.

Staff, learners and other authorised users are responsible for good behaviour on the College Network system just as they are throughout the College.

The Internet is provided for staff, learners and other authorised uses to communicate with others and conduct research relevant to their course of study or duties. Please remember access is a privilege, not a right and that access requires responsibility.

Individual users of the Internet are responsible for their behaviour and communications over the network. It is presumed that users will comply with College standards and all relevant legislation.

Southern Regional College reserves the right to deny or limit computer usage and related services to groups or individuals. Co-operation by staff, learners and other authorised uses is essential if the College is to adequately serve all its customers. Staff, learners and other authorised users who refuse to co-operate with College personnel enforcing the Acceptable Use Policy will lose the right to use the computer network services and will be subject to appropriate disciplinary procedures.

5. DISTRIBUTION

MLE
All Staff and Learners

6. RELATED DOCUMENTS

Data Protection Policy
Network Security Policy
College Equal Opportunities Policy
JANET Acceptable Use Policy
Harassment Policy
Safeguarding Policy
Social Media Policy
Portable Media Policy

Acceptable Use Policy Statement of Compliance – Learners
Acceptable Use Policy Statement of Compliance – Staff
Acceptable Use Policy Summary

Human Rights Act 1998 (HRA)
Data Protection Act 1998 (DPA).

7. FLOW CHART

None

Network Acceptable Use Policy

Learner Statement of Compliance

Name: _____

Class : _____

My Lecturer has taken me through the College's Network Acceptable Use Policy. I fully understand the terms and conditions of this policy and agree to abide by it. I realise that the College's security software may record for management use the Internet address of any site I visit and keep a record of any network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive may be recorded and stored in an archive file. I know that any violation of this policy may lead to disciplinary action being taken.

Learner Signature: _____

Date: _____

The full version of this Policy is available on the College's MLE.

Network Acceptable Use Policy

Staff Statement of Compliance

Name: _____

National Insurance Number: _____

Username(s): _____
(Only applicable if you have a Username)

Department: _____

Line Manager's name _____

I have read the College's Network Acceptable Use Policy. I fully understand the terms and conditions of this policy and agree to abide by it. I realise that the College's security software may record for management use the Internet address of any site I visit and keep a record of any network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive may be recorded and stored in an archive file. I know that any violation of this policy may lead to disciplinary action being taken.

Staff Signature: _____

Date: _____

The full version of this Policy is available on the College's MLE.

PLEASE RETURN COMPLETED VERSION TO HUMAN RESOURCES, NEWRY CAMPUS, WEST BUILDING

NETWORK ACCEPTABLE USE POLICY SUMMARY

SUMMARY POLICY STATEMENT

The Network Acceptable Use Policy is designed to outline for staff, learners and other authorised users the conditions of use for these resources so that all users can benefit from the facilities.

General Principles

- All staff and learners of Southern Regional College are permitted and encouraged to use the College's ICT facilities, including the public Internet, provided that the conditions of use are adhered to.
- The Internet and Intranet are to be used in a manner that is consistent with the College's standards.
- The facilities are to be used as part of the normal execution of a learner's education, a lecturer's instruction or an employee's job responsibilities.
- Users should be aware that all data on the network will be monitored. This includes e-mail messages and any data on media connected to College facilities. College supplied e-mail addresses are not private. Neither should a user assume that the information systems are secure.
- All web content must be sanctioned by the appropriate authority before being published. Recipients of transmitted information should be informed that opinions expressed by individuals are not necessarily those of the College.

Unacceptable Practices

The following practices are unacceptable and may be subject to disciplinary action, including revocation of access privileges, written warnings, termination of employment and in some cases, reporting to the police.

- The creation or transmission (e.g. by visiting an Internet site) 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.
- The creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- Uploading, downloading or otherwise transmitting commercial software or copyrighted material in violation of its copyright.
- Representing personal opinions as those of the College.
- Using the College's resources (including Internet and e-mail) for profit or private gain.
- Downloading any software or electronic files without implementing virus protection measures that have been approved and/or prescribed by the College.
- Hacking in any form. Intentionally interfering with normal operation of the network, including propagation of viruses, by-passing filtering systems, or sustained high volume network traffic;
- Examining, changing or using another person's files, output or username without explicit permission.
- Revealing or publicising confidential or proprietary information, which includes, but is not limited to: College databases, personal user information, access codes, computer software.
- Using the network for non-educational or non-scholastic purposes.
- The transmission of unsolicited material to other users, organisations or networks.
- Deliberate unauthorised access to facilities or services accessible via the network.
- Installation of software, except with the express permission of ICT Support.