NETWORK ACCEPTABLE USE POLICY

Process Area	**ICT**
Reference Number	**ICT/001**
Directorate	**Finance and Planning**

Issue No	Date	Details	Author	Approved
001	Feb 2008	First Issue	ICT MG	SMT
002	Jan 2013	Updates to all sections	S Todd	SMT
003	Jan 2014	Reviewed – no updates to text, new logo added.	JO'H	BD
004	Jan 2017	Reviewed minor updates to learner requirements applied	S Todd	Governing Body
005	Dec 2019	Reviewed to separate policy and procedural note	ST/TMG	Governing Body F&GP
006	Oct 2022	Included references to College's Privileged User Charter and added a Statement of Compliance for Guest Users. Procedural note merged into the policy	LC, ST	Governing Body F&GP

If requested, the College will make the policy available in alternative formats to accommodate visual impairments. The policy can also be downloaded from the College website and made available in alternative languages upon request.

1. POLICY STATEMENT

All users of the College ICT Systems and Services are bound by this policy at all times when using equipment, software or services provided by the College.

The College will provide access to a range of information technology resources to assist teaching and learning, research and information handling. In addition, teaching and support staff will have controlled access to a range of business support applications. This represents a considerable commitment of College resources in the areas of telecommunications, networking, software and storage. It is important that there are rules in place that define what is deemed acceptable in order to ensure that the College's IT resources are not misused in anyway.

The purpose of this Policy is to:

- Outline for staff, learners and other authorised users the acceptable and unacceptable use of these resources.
- To protect the College, it's students, staff, partners and those using our ICT facilities from illegal, inappropriate or damaging actions.
- To ensure resources are used in an appropriate manor allowing users to be more productive and effective in their use. The primary use of College ICT facilities should be for academic and business purposes.
- To ensure the availability of systems and services for all users and prevent impact through inappropriate or damaging actions.
- To outline how the College will respond to any potential breaches of these rules.

2. SCOPE

This policy applies to all authorised Users of College IT resources (see definition below).

This policy applies to all areas of the College network, associated IT systems and information.

The College IT networks are connected to other educational institutions and to the rest of the internet via JANET, the electronic communications network and associated electronic communications and networking services and facilities that support the requirements of the UK education and research communities. Acceptance of this College Policy is deemed to be acceptance of the JANET Acceptable Use Policy (https://community.ja.net/library/acceptableuse-policy).

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.
Section Managers (Information Owners)	These are usually the Head of Department with responsibility for the information contained within their department.
User	Any person who operates, has access to or interfaces with IT. This includes College employees, workers and Governing Body members, students, contractors, sub-contractors, consultants, business partners, official visitors or customers of the College.
Privileged user	Any user who has been provided with elevated access permissions to Physical, Systems and Information.

4. ROLES AND RESPONSIBILITIES

4.1 Chief Executive and Director of Finance and Planning

The Chief Executive and Director of finance and planning shall:

- have overall responsibility for the development, review and monitoring of this policy on a continuing basis.

4.2 Assistant Director for ILT Development and ILT Systems

The Assistant Director for ILT Development and ILT Systems is responsible for:

- ensuring that users of College ICT systems follow and adhere to good practice in relation to the use of ICT. The policy forms the basis of a framework of policies regarding the use of ICT system and information security.

4.3 Section Managers (Information Owners)

Section Managers with specific 'Line of Business' applications within their department must ensure:

- that this policy is applied to the use of systems within their responsibility; and
- be aware of their responsibilities as an information owner and ensure appropriate controls are in place to protect the information they are responsible for.

4.4 Head of ICT and Network Systems

- The Head of ICT and Network Systems must ensure that this policy is applied.

- Ensure any monitoring of ICT system is completed in compliance with UK legislation.
- Ensure appropriate guidance is issued on the acceptable and unacceptable use of ICT Systems.

4.5 Privileged Users

Privileged Users shall abide by the College's Privileged User Charter and only use elevated access in line with the purpose for which it has been allocated.

4.6 Users

- Acceptable use of the College's information systems & facilities is defined as their use for the College's teaching, learning, research and administrative activities. For students, this includes research and assignment work. For staff, this includes administrative, teaching and research activities.
- Users must act in accordance with UK law, and material imported or transmitted across international boundaries must not contravene international laws or treaties.
- Users must not carry out any activity identified as unacceptable as defined with the Network Acceptable Use Policy.
- All users must be familiar with relevant College policies and procedures and take note of guidance on security as issued by IT Services. Failure to conform to these requirements may lead to suspension of account privileges or other disciplinary action as appropriate.
- Any suspected breach or misuse of a user account should be reported immediately to your line manager or head of faculty and IT Services.
- Any damage, loss or theft of College IT must be reported immediately to your line manager or head of faculty and IT Services.
- Individual users of the Internet are responsible for their behaviour and communications over the network.
- Users must treat equipment issued to them with due care and respond appropriately to requests relating to maintenance or return.
- Follow any guidance issued by IT Services relating to use of IT Services.
- Occasional and moderate use of college information systems facilities for private use is permitted, provided it does not occupy class time or the employer's time, and does not entail trading or selling. College e-mail address must not be provided in relation to the private use of any on-line service.
- On-going use of computing facilities by users constitutes acceptance of the Acceptable Use Policy.
- Users may be held personally liable for the consequences of misuse. Where misuse is illegal or unlawful, or results in loss or damage to College resources or the resources of third parties, the matter may be referred for legal action.
- Where necessary, on violation of the policy, services may be withdrawn from a user. Breach of this policy will be referred for appropriate disciplinary action.
- Users must respect the rights of other computer users, respect the integrity of physical facilities and controls, and respect all licence and contractual agreements related to College IT systems. All users must act in accordance with these responsibilities, and the relevant local, national and international laws where applicable.

- 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.

- Users are expected to practise sensible use to limit wastage of College IT resources or bandwidth. This includes avoiding unnecessary printing, and unnecessary Internet access, uploads or downloads.
- All College IT should be cared for in a responsible manner. All food, drink, chewing gum etc. must be kept away from IT.

The following activity is considered unacceptable use:

- Use College IT resources to operate a business or participate in any pursuit geared to personal gain for themselves or an associate.
- Cause College IT to become unusable or inaccessible to other Users through abuse or misuse.
- Intentionally jeopardise the security of any College IT.
- Any form of cyberbullying;
- Creation or transmission or causing the transmission of any offensive, obscene, hateful or other objectionable materials;
- Creation or transmission of material with the intent to defraud or assist criminal activity, e.g. Phishing;
- Creation or transmission of defamatory material;
- Creation or transmission of unsolicited bulk or marketing materials to other users;
- The use of the College's information systems to cheat, plagiarise or steal the work of others;
- 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;
- Hacking in any form;
- Deliberate avoidance or bypassing of network monitoring and security measures (e.g. proxy sites);
- Operating a business over the College's information systems facilities without permission;
- Where the JANET Infrastructure is being used to access another network, any violation of access policies of that network will be regarded as unacceptable use of JANET;
- Reveal, publicise, theft or destruction of 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 username for which they do not have explicit authorisation;

- Use other network facilities for excessive personal use unrelated to College business. Network storage areas and removable media will be viewed as College property. The Head of IT and Network Systems or their 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 without the expressed permission of ICT Support;
- Connect any networkable device to the College's networks without the approval of ICT Support. The sole exception to this is the eduroam Wi-Fi service provided by the College;
- Deliberate activities with any of the following characteristics:
    - wasting staff effort or networked resources
    - corrupting or destroying other users data
    - violating the privacy of other users
    - disrupting the work of other users
    - denying service to other users (for example, by deliberate overloading of systems)
    - continuing activities that the college has requested to cease because it is causing disruption to services.
    - the introduction of "viruses" or other harmful software. Any other use deemed unacceptable by supervisory staff.
    - Perform any other inappropriate uses.

5. GENERAL PRINCIPALS

By using College IT resources, the user has personal responsibility for their appropriate use and agrees to comply with this policy and other applicable College policies and all relevant laws and regulations. This will help to ensure the security, confidentiality and safety of the College's IT resources.

Access to IT resources at the College is a privilege, not a right, and all users must act honestly and responsibly.

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.

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 and may be treated as a serious disciplinary issue. 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 ICT Systems are minimised and that users are made aware of what is deemed acceptable use of network resources. The College will deploy software to block access to inappropriate and illegal material on the Internet from all sites that it knows about. These sites constantly change, and IT cannot guarantee to block access to all such sites at any one time.

Data transmitted or received using College IT systems may be stored by the College and may be used by the College in ensuring it can enforce relevant legislation.

6. CONTROLS

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 College will implement several controls to protect both the College and its ICT System users. These will include:

Technical Controls - The College will implement a range of technical measures such as Firewalls, IPS/IDS, End point security, web filtering solutions etc.

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 this Policy. All users will be expected to accept this Policy and staff will sign a statement of compliance. Learners agree as part of their enrolment terms and conditions to abide by this Policy.

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.

7. IT RESOURCES

- While the use of information and communication technologies is a required aspect of the College's academic programmes, access to the College IT systems remains a privilege and not a right. It is given to students and staff who act in a considerate and responsible manner and shall be withdrawn from those failing to maintain acceptable standards of use.

- Users must not attempt to gain access to any IT resource that they are not authorised to access. This includes but is not limited to manual and electronic records/data, applications/programs, facilities and buildings.
- Each user is responsible for the security of any College owned information resource in their possession (this includes but is not limited to computer equipment, network accounts, telephone/voicemail accounts and electronic and manual data, confidential or otherwise).
- The College believes that computing resources should be available on as wide a basis as possible.
- All computers connected to the College's networks, whether owned by the College or not, must have an approved, up to date virus-scanning software running in-line with the relevant policy.

8. 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.
- Each user is responsible for all activities which originate from any of their accounts.
- All users are required to use Multi factor authentication if accessing Network Services remotely.

9. USE OF LRC AND ANY OPEN ACCESS FACILITIES

- Staff, learners and other authorised users 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.
- 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 Learning Resource Centre.

10. POLICY BREACH

- If any user is found to have breached this policy or any related policy, they will be dealt with in accordance with the College’s relevant disciplinary procedure. This form of action may lead to termination of employment for employees; termination of a contract in the case of service providers, consultants or temporary staff and expulsion in the case of a student.
- It is a condition of computer systems usage that all users abide by the terms and conditions of this Policy. The use of IT resources and electronic communication equipment must always be consistent with the College’s statutory obligation in which to maintain the highest ethical standards.

- If a breach of this policy has the potential to be of a criminal nature, the College reserves the right to refer the matter to the relevant authority.
- If users do not understand the implications of this policy or how it may apply to them, they can seek advice from their line manager, Human Resources or the IT Helpdesk.

11. MONITORING

The College respects the privacy and academic freedom of staff and students. However, the College may carry out lawful monitoring of ICT systems. Staff, students and any other authorised users should be aware that the College may access documents, email, telephone and any other electronic communications, whether stored or in transit. This is in order to:

- comply with the law and applicable regulations;
- to ensure appropriate use of the College ICT systems and to prevent or detect misuse;
- in the interests of security;
- to investigate or detect unauthorised use of networked systems;
- to secure effective system operation;
- in association with specialist training.

All access and monitoring will comply with UK legislation as identified in related documents.

12. DISTRIBUTION

- SharePoint Policy Centre
- College Web Site

13. RELATED DOCUMENTS

- FE Sector Data Protection Policy (UK GDPR)
- ICT Network Security Policy
- Equality and Good Relations Policy
- JANET Acceptable Use Policy (JISC)
- Harassment Policy
- Safeguarding Policy
- Social Media Policy
- Information Handling Policy
- Network Acceptable Use Policy Statement of Compliance – Staff
- Mobile and Remote Working Policy
- Bring your own Device Policy

Applicable laws, primary Acts of Parliament and policies which relate to and/or govern the provision and use of IT facilities include:

- Regulation of Investigatory Powers Act 2000
- Computer Misuse Act 1990
- Data Protection Act 2018

- UK General Data Protection Regulations (UK GDPR)
- Freedom of Information Act 2000
- Copyright, Designs & Patents Act 1988
- Copyright and Trademarks (Offences and Enforcement) Act 2002
- The Telecommunications Act (1984)
- The Electronic Communications Act (2000)
- Obscene Publication Act 1959 & 1964
- Protection of Children Act 1978
- The Defamation Act (1996 and 2013)
- Police and Criminal Evidence Act 1984
- Police and Justice Act 2006
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Counter Terrorism and Security Act 2015
- Human Rights Act 1998
- Equality Act 2010
- Privacy and Electronic Communications Regulations 2003

** This list is not exhaustive and will be subject to change **

14. FLOW CHART

None.

15. APPENDICIES

Appendix 1 - Statement of Compliance (Staff)
Appendix 2 - Statement of Compliance (Guest)

Appendix 1 - Network Acceptable Use Policy

Statement of Compliance (Staff)

Name:	
National Insurance Number:	
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 Policy Centre.

PLEASE RETURN COMPLETED VERSION TO
HUMAN RESOURCES,
NEWRY CAMPUS.

Appendix 2 - Network Acceptable Use Policy

Statement of Compliance (Guest)

Name:	
Organisation:	

By using college ICT facilities, I agree to abide by College rules and guidance on their use. 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 will lead to access being revoked.

Signature:		Date:	

The full version of this Policy is available on the College's Intranet and website.