South Staffordshire College

Lichfield • Cannock • Tamworth • Rodbaston

IT Conditions of Use (Operational Policy)

Reference: Version	1
Policy Originator:	Jamie E Smith
Equality Impact Assessed:	Yes
Approved by:	SLT
Date Approved:	19/10/15
Review Interval:	2 Year Cycle
Last Review Date:	2015
Next Review Date:	2017
Audience:	All-staff & Learners

Reference: Version	1
Policy Originator:	Jamie.E Smith
Equality Impact Assessed:	Yes
Approved by:	SLT
Date Approved:	19/10/15
Review Interval:	2 Year Cycle
Last Review Date:	2015
Next Review Date:	2017
Audience:	All-staff & Learners

South Staffordshire College

Lichfield • Cannock • Tamworth • Rodbaston

IT Conditions of Use (Operational Policy)

1.0 Purpose

1.1 The purpose of the IT Conditions of Use Regulations are to define acceptable use of College IT systems, hardware, telephone and wider technology.

1.2 These regulations will support the implementation of our "Purpose":

"*Transforming the life chances of our communities.*"

It will achieve this through a best endeavour to deliver a safe and secure digital environment for the purpose of enhancing learning.

2.0 Scope

2.1 These regulations apply to all staff and learners within the college as well as visitors, contractors and anyone making use of the college IT systems and infrastructure, irrespective of location and covers all devices, systems and infrastructure at all times.

2.3 Key linked policies include the college Digital Professionalism Policy, Data Protection Policy, E-Safety Policy and Safeguarding policy and procedures.

3.0 Statutory Framework

The primary legislation relating to these regulations include:

- **Regulation of Investigatory Powers Act 2000.**
- **The JaNET Acceptable Use Terms and Conditions.**
- **The Data Protection Act.**
- **The Freedom of Information Act.**
- **Copyright legislation.**
- **Defamation.**
- **Obscene publications.**
- **Discrimination legislation.**

4.0 General

4.1 When using IT systems, you remain subject to the same laws and regulations as in the physical world. It is expected that your conduct is lawful. Ignorance of the law is not an adequate defence for unlawful conduct.

4.2 You must abide by the regulations applicable to any other organisation whose services you access such as JaNET.

4.3 Some software applications provided by the college may have their own regulations for the user – these should also be adhered to.

4.4 The IT facilities are provided for use in furtherance of the purpose of the college, for example to support a course of study, research or in connection with your employment by the institution.

4.5 Reasonable use of IT facilities for personal activities (provided that it does not infringe any of the regulations, and does not interfere with others' valid use) is permitted. Use of these IT

facilities for non-institutional commercial purposes, or for personal gain, requires the explicit written approval of the Director of Strategy & Infrastructure.

4.6 You must take all reasonable precautions to safeguard any IT credentials issued to you. You must not allow anyone else to use your IT credentials (login, passwords). Nobody has the authority to ask you for your password and you must not disclose it to anyone. You must not attempt to obtain or use credentials assigned to someone else. You must not impersonate someone else or otherwise disguise your identity when using the IT facilities.

4.7 You must not do anything to jeopardise the integrity of the IT infrastructure by, for example, doing any of the following:

- Damaging, reconfiguring or moving equipment.
- Loading software on the college equipment other than in approved circumstances.
- Reconfiguring or connecting equipment to the network.
- Setting up servers or services on the network.
- Deliberately or recklessly introducing malware or any software that could be considered hostile.
- Attempting to disrupt or circumvent IT security measures.

5.0 Information

5.1 If you handle personal, confidential or sensitive information, you must take all reasonable steps to safeguard it and must observe the relevant guidelines associated with handling information under the Data Protection Act. Ignorance of the law and associated good practice in handling information is not an acceptable mitigation.

5.2 You must not infringe copyright, or break the terms of licences for software or other protected material.

5.3 You must not attempt to access, delete, modify or disclose information belonging to other people without their approval to do so.

5.4 You must not download, create, store or transmit unlawful material, or material that is indecent, offensive, threatening, discriminatory or extremist. You should be aware that just the

viewing of material that falls into these categories can be regarded as an offence and can have serious consequences. The use of 3G/4G or future mobile communications standards should not be used to access extremist or inappropriate material whilst on College premises

5.5 You should be aware and informed of the 'Prevent' policy and agenda and play a proactive role in ensuring that its guiding principles are upheld and promoted at all times. The College Safeguarding policy is available via the intranet and a range of wider CPD material is also available.

6.0 Behaviour

6.1 Appropriate standards of behaviour expected in the physical world apply equally in a digital one, especially in regard to social media.

6.2 The College encourages the appropriate use of social media technologies as a tool to support engagement in learning and teaching. However you must not cause needless offence, concern or annoyance to others in using these technologies.

6.3 You must not deliberately or recklessly consume excessive IT resources such as processing power or network bandwidth. You must not use the IT facilities in a way that interferes negatively with wider valid use.

7.0 Monitoring

7.1 The College monitors and records the use of its IT facilities for the purposes of:

- The effective planning and operation of the IT infrastructure.
- Detection and prevention of infringement of these regulations.
- Investigation of alleged misuse.

7.2 The College will comply with lawful requests for information from government and law enforcement agencies.

7.3 You must not attempt to monitor the use of the IT facilities without explicit authority from the Director of Strategy and Infrastructure.

8.0 Infringement

8.1 Infringing these regulations may result in disciplinary action.

8.2 Penalties may include withdrawal of services and wider action being taken.

8.3 Offending material will be taken down. Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations whose regulations you have breached.

8.4 South Staffordshire College reserves the right to recover from you any costs incurred as a result of your infringement. You must inform the Director of Strategy and Infrastructure if you become aware of any infringement of these regulations.

9.0 Liability

9.1 The College has no obligation to retain a user's IT resources after their authorisation has ended.

9.2 The College will not accept any liability for loss or corruption of information held, or for damages, injury to third parties, economic loss whether caused by negligence or otherwise, or expenses which may result from the use of IT or withdrawal at any time of such facilities by the college.

9.3 The College reserves the right to take legal action against an individual who causes it to be involved in legal proceedings as a result of a breach of these regulations and to seek reimbursement of any consequent damages, costs or other expenditure awarded against the college or incurred by it.