South Tyneside College
Dedicated to your success

E- SAFETY POLICY

This policy is available on-line at: www.stc.ac.uk

- We will consider any request for this policy to be made available in an alternative format or language. Please contact: Student Services Coordinator
- We review our policies regularly to update them and to ensure that they are accessible and fair to all. We welcome suggestions for improving the accessibility or fairness of this policy.
- All our policies are subject to equality impact assessments*. We are always keen to hear from anyone who wishes to contribute to these impact assessments. Please contact: Student Services Coordinator

*Equality Impact Assessments are carried out to see whether the policy has, or is likely to have, a negative impact on grounds of: age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex or sexual orientation.

Approved by:	Version:	Issue Date:	Review Date:	Contact Person:
SEG	v.3	March 2017	April 2020	Head of IT & Soft Services

Equal Opportunities: **Impact Assessed**

Review:

POLICY NUMBER 22

E- SAFETY POLICY

1 Policy Statement

South Tyneside College is committed to providing a safe environment for the use of IT.

E-Safety is about applying the lessons we have learnt about keeping children, young people and adults safe to technology. E-Safety must be responsive to new technologies and new threats and opportunities that may arise.

E-Safety, is not technical in nature, it is not about virus protection, internet filtering, firewalls or other IT security concerns. E-Safety is about ensuring that technology is used in a manner that is safe and respectful to others. Due to this E-Safety has a significant overlap with other policies and procedures, particularly those related to child protection, anti-bullying and acceptable use of IT.

2 Scope

An e-safety incident is considered to have occurred when a learner, staff member or Governor instigates, or is the victim of, an activity which utilizes Information and Communications Technologies (IT) to endanger the personal safety, mental well being, or financial well being of another individual.

Activities which will be considered e-safety incidents include, but are not limited to, the use of ICT to

- Access, view, copy or download illegal content, or materials, including, but not limited to:
    - child pornography
    - materials inciting racial hatred or violence
- Access, view, copy or download inappropriate content, or materials, as defined by the College's Acceptable Use of IT policy.
- Bully or harass an individual or group (Cyber Bullying).
- Commit fraud or identify theft.
- Undertake any activities which would be in violation of the Child Protection, Protection of Vulnerable Adult or Anti-Bullying policies
- Any other incident where it can be reasonably considered that the personal safety, mental well being or financial health of an individual has been endangered by the use of ICT.

In this context ICT includes, but is not limited to,:

a) College owned equipment, including:
    - Desktop PC's
    - Servers
    - Laptop/Tablet devices
    - Telephones, both fixed and mobile
    - Digital video camera or camcorders
    - Digital audio recording devices
    - Reproduction devices (scanners, printers, etc..)
    - Any and all software and IT services provided by the College

b) Privately owned ICT equipment (including personal mobile phones), when:

- Connected to any College owned network
- Utilised to access College software and services
- Made use of on campus, or in the pursuit of College business.

3 Legislation

- Computer Misuse Act 1990
- Data Protection Act 1998
- Malicious Communication Act 1998

4 Responsibilities

4.1 All staff have a responsibility to give full and active support for the policy by ensuring:

4.1.1 The policy is known understood and implemented.

4.1.2 All actual and suspected serious e-Safety incidents are reported to a designated safeguarding manager

Parents/Guardians, providers, sponsors, employers and other stakeholders have a responsibility to report any e-Safety concerns they may have to the College.

4.2 Individual learners have a responsibility to:

4.2.1 Report any e-Safety concerns they may have to any member of staff that they feel comfortable with.

4.2.2 Refrain at all times from any behaviour which would result in the occurrence of an e-Safety incident.

5 Actions to Implement and Develop Policy

5.1 Reporting

Serious e-Safety incidents should be reported to a designated safeguarding manager who will log the incident in the safeguarding database.

5.2 Securing and Preserving Evidence

IT Services should be contacted immediately following the reporting of any serious e-Safety incidents and asked to make copies of relevant access logs, files etc…

If it is believed that an immediate risk of exposure to illegal or inappropriate materials, or mental distress exists to staff or learners, the computer or devices should be turned off immediately. **You should not "shutdown" or log off as this may corrupt, delete or overwrite evidence, the power supply should be turned off at the wall or the battery should be physically removed.**

The equipment should then be moved to a secure location.

5.3 Illegal Material or Activities

Unless it is considered that an immediate danger exists to learners, staff or the public, no action should be taken which will alert the suspected individual(s).

The person discovering the activity should immediately and discreetly inform the Head of IT Services (or nominated deputy).

The Head of IT Services is responsible for involving other senior managers and law enforcement agencies as required. IT Services will assume responsibility for obtaining, securing and preserving appropriate additional evidence. For example, remote screen shots, web filter logs etc.

If it is believed that a child protection issue exists the procedures outlined in the Child Protection Policy should be enacted.

5.3.1 Child Pornography

If it is suspected that an individual may have been accessing child pornography the power supply, or battery, should be physically removed from the device immediately.

Under no circumstances should any person make copies, including screen dumps or print outs, of suspected child pornography. Taking copies of such materials, even when intended for evidentiary purposes, is a crime.

5.4 Inappropriate Material or Activities

Inappropriate material or activities are considered to be any materials or activities which are considered as unacceptable by the Acceptable Use of IT policy.

5.4.1 Staff Access to Inappropriate Material

Where it is suspected that a staff member has been accessing inappropriate material the time and date of the incident should be noted and the concerns raised with the individual's line manager.

5.4.2 Student Access to Inappropriate Material

Where it is suspected that a learner has been accessing inappropriate material the time and date of the incident should be noted and brought to the attention of the relevant Curriculum Leader or Head of School. The IT Helpdesk should also be contacted and asked to take copies of relevant access logs etc…

5.5 Cyber-Bullying

Cyber-Bullying can be defined as making use of IT to undertake to bully. Examples of cyber-bullying include, but are not limited to:

- Sending offensive or abusive e-mails, instant messages, or “text” messages.
- Inviting selected individuals to a chat room or website to discuss another individual who has not been invited.
- Posting offensive, defamatory or abusive messages about an individual or group to a public or members only internet forum.
- Using a digital camera to take humiliating images

Incidents of actual or suspected cyber-bullying should be dealt with in accordance with the Anti-Bullying policy.

5.6 Virus & Malware Protection

Anti-virus and anti-malware software is installed on all College systems. This software provides an important line of defence against some forms of cyber-crime, in particular identity theft.

IT Services will make all reasonable efforts to ensure current, up to date, anti-virus and malware protection is installed on all College systems. However, users of the systems have a responsibility to:

- Alert IT Services if they discover a fault with their anti-virus and anti-malware software

- Ensure personally assigned devices (i.e. laptops) are connected to the network at least once per month.

5.7 Training

Provide mandatory training to all staff on e-Safety awareness and their responsibilities in the event of an e-Safely incident.

6 Related Policies

- **Data Protection Policy**
- **Anti Bullying Policy**
- **Acceptable Use of IT Policy**
- **Control of IT Hardware and Software Policy**
- **Safeguarding Policy**
- **Disciplinary Procedure**