South Staffordshire College

E-SAFETY POLICY

Reference: Version	V3
Policy Originator:	Assistant Principal – Learner Services
Equality Impact Assessed:	July 2019
Approved by:	Governors
Date Approved:	July 2019
Review Interval:	2 years
Last Review Date:	April 2019
Next Review Date:	July 2021
Audience:	Staff, Learners, Governors, Stakeholders

Admissions Policy

1.0 Policy Statement

1.1 This policy articulates the commitment of South Staffordshire College to support all stakeholders to be vigilant and remain safe whist using online technology. The college promotes e-safety as a part of the overall safeguarding support available on campus.

1.2 The policy will establish clear guidance regarding staying safe in online spaces and establish key principles, structures and monitoring arrangements for the college.

1.3 This policy will support the implementation of our vision:

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

2.0 Scope

2.1 The scope of this policy outlines all the procedures and processes of the college relating to the legal observation and promotion of online safety.

2.2 This policy applies to all learners, staff, governors, contractors, clients, business partners, volunteers and visitors with whom we work to deliver services.

2.3 Policies linked this include:

- Learner Conduct
- Safeguarding Policy
- Safeguarding Procedures
- IT Conditions of Use
- Digital Professionalism
- General Data Protection Regulation (GDPR)

2.4 Raise the awareness of all staff and learners that the college's legal duty to safeguard children and vulnerable adults extends to both the college's physical and virtual environment. This involving electronic communications such as the intranet, mobile phones and other forms of technology.

2.5 Support staff in safeguarding learners as well as safeguarding themselves in respect of electronic communications.

2.6 Help staff to understand the implications of their legal duty and ethical responsibility in identifying and reporting suspected or known e-safety issues, which may include the abuse or neglect of a child or vulnerable adult.

2.7 Identify strategies to minimise risks posed by electronic communications and to promote safe practices in the use of electronic communications including the internet, social networking sites and mobile phones.

2.9 Ensure that all allegations of abuse are appropriately and effectively handled.

2.10 Support the development of effective working partnerships with other agencies, including the Police, Child Exploitation and Online Protection Agency (CEOP), Staffordshire Safeguarding Children Board (SSCB) and Entrust.

2.11 To establish the appropriate procedures for addressing complaints regarding e-safety.

2.12 To reinforce ICT acceptable use policies for learners and staff and other related policies.

3.0 2025 Vision and Strategic Objectives

3.1 This policy will be implemented in a manner that embraces our "Values" and "Guiding Principles:

Guiding Principles:

- Excellence in learning and teaching
- Community contribution
- Entrepreneurial attitude

Values:

- *Togetherness* - Working together to provide an outstanding experience for our learners, employers and communities
- *Standards* - High performance to enhance life chances and success of learners, communities and employers
- *Sustainability* - A beacon for sustainable development, to educate, inspire and enhance quality of life
- *Customer Care* - Exceed the expectations of all by providing creative leadership, inclusivity and respect for people and their future

3.2 All decisions based on admissions will contribute to the meeting of the College's overall strategic priorities:

- Increase participation
- Deliver outstanding teaching, learning and business services
- Deliver excellence
- Develop a highly engaged and skilled workforce
- Achieve financial stability and improve efficiency

4.0 Key Principles

4.1 The Policy will be implemented in accordance with all existing and emerging legislation.

4.2 The Policy will be publicised as widely as possible to include staff, learners, governors, business partners and the community and will be available in a variety of formats on request.

4.3 South Staffordshire College aims to create and maintain a safe and welcoming environment, both physically and virtually, for all learners, staff, governors and visitors.

4.4 Electronic communication tools such as the internet and mobile phones can enhance learning and social development opportunities for both learners and staff. However, the use of electronic communications also poses risks as the technology may be used for a range of negative, highly damaging and potentially illegal activities including privacy invasion, cybercrime, cyberbullying and educational misconduct.

4.5 The former British Educational Communications and Technology Agency (BECTA) summarised the risks posed by electronic communications under four key headings:

A. E–Safety Content

a. Exposure to age inappropriate material such as games and film clips
b. Exposure to inaccurate or misleading information
c. Exposure to socially unacceptable material such as that inciting violence, hatred or intolerance
d. Exposure to illegal material such as images of child abuse

B. E–Safety Contact

a. Grooming using communication technologies, social networking sites and chat rooms
b. Risks attached to sharing personal information and identity theft

C. E–Safety Commerce

a. Exposure of minors to inappropriate commercial advertising
b. Exposure to online gambling services
c. Commercial and financial scams

D. E–Safety Culture

a. Bullying via websites, mobile phones etc.
b. Illegal downloading of copyright material
c. Plagiarism
d. Reduced concentration and increased distraction in the learning environment

4.6 South Staffordshire College, guided by the policies and procedures of SSCB, is committed to adopting early intervention strategies to help to reduce the risk of and to prevent 'significant harm' to young people and 'serious harm' to vulnerable adults.

4.7 The college fully recognises its responsibility to protect and promote the safety and well-being of young people. We are proactive in our duty to work with other agencies in order to achieve this and have a highly positive approach to multi-agency working.

4.8 The college recognises that every staff member has a legal duty to report cases of suspected abuse, no matter how small or trivial they may seem. We acknowledge that young people may be subject to abuse, which can include physical, emotional, financial, sexual or neglect, placing them at risk of significant or serious harm and exploitation.

4.9 All allegations of abuse will be taken seriously and treated in accordance with the college's Safeguarding Procedures which are informed by effective and thorough risk assessments.

4.10 The college is required to have a Designated Safeguarding Lead (DSL), who is responsible for ensuring that any disclosures or suspicions of abuse are reported to the

appropriate agency. The Assistant Principal – Learner Services, is the College's DSL and supported by the Safeguarding Team.

4.11 The College is committed to supporting, resourcing and training those who work with, or who come into contact with children in order to ensure appropriate supervision and care.

5.1 **Definitions**

5.1 For the purposes of the E-Safety Policy:

- A 'child' is a young person under the age of 18 years
- An adult is a person aged over 18 years of age
- A 'vulnerable adult' is, *"A person who is 18 years of age or over, and who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of him/herself, or unable to protect him/herself against significant harm or serious exploitation."*
- Reference to 'staff' includes all employees who are full-time, part-time, variable hours, agency, franchise, contract and volunteer staff working for the college.

5.2 The college recognise that an adult may become vulnerable at any time due to a range of circumstances such as a bereavement or drugs and alcohol misuse. In so doing, we recognise that this Policy has relevance to many adult learners, whom we will seek to protect and support in accordance with the Safeguarding Procedures.

5.3 Any concern for 'significant harm' must be judged on a case by case basis as there is no one absolute legal definition. Issues to consider in judging whether the threshold of significant harm has been met include the degree and extent, duration and frequency of harm and whether it was premeditated.

5.4 There are four important elements to creating an e-safe environment, illustrated by the 'PIES model' consisting of:

- P - comprehensive **p**olicies supported by consistent e-safety **p**ractices
- I - a safe and secure technology **i**nfrastructure
- E - **e**ducation and training for all members of the learning community
- S - **s**tandards and inspection

6.0 Practices to Promote E-safety

6.1 Induction and training

Staff and learners will be introduced to this policy during their induction to the college. For staff, this will form part of their Level 1 Safeguarding training, which they will repeat at least once every three years. Managers are responsible for signing off members of staff who have successfully completed their probationary period.

For learners, this will be introduced during the Induction period, when learners are reminded of our commitment to safeguarding their health and well-being in its broadest

sense. Learners will sign to confirm they understand and will abide by the college's policies, including this Policy and all those specifically linked to it, including the College's IT Conditions of Use Policy which details appropriate use of IT in College.

6.2 E-safety Promotion

The college will regularly promote staying safe to learners throughout the tutorial programme. In addition, e-safety will be embedded within curriculum delivery, with reiterative promotional messaging used in Learning Resource Centres (LRC) and the college's website and official social media outlets. Using intelligence gleaned from learners and staff, e-safety promotion will also be targeted at individuals or groups whom are known to be particularly vulnerable. The Mentoring and Safeguarding Team will provide particular support with this.

7.0 E-Safety and the College Infrastructure

7.1 College Safeguarding Team

The College Safeguarding Team meets termly to review and improve issues related to safeguarding learners and staff, including e-safety. Regular and timely reports will be made available for relevant committees.

7.2 Online Activity

Learners and staff are encouraged to make positive educational use of the internet. The college deploys virus protection technology to ensure the security of the network. In addition, filters are used to minimise the risk for staff and learners to be accidentally exposed to inappropriate or illegal content, or from downloading such materials deliberately. Browser settings on the college internet are set to minimise the likelihood of accessing inappropriate sites such as gambling sites or sites that may include inappropriate images.

Breaches of this policy can result in system usage rights removed and are subject to the relevant disciplinary procedures. Internet usage rules are contained in the College's IT Conditions of Use Policy. Regular checks are made by IT staff to ensure that the filtering methods selected are appropriate, effective and reasonable and do not inhibit the college's ambition to fully exploit the internet for high quality teaching and learning.

7.3 Social Networking

The college uses social media to share information and gather opinions from its stakeholders including learners, parents/carers, staff and customers. The college social media accounts are monitored by the Marketing team and inappropriate material or comments are removed.

Social networking sites can be valuable educational resources. The college takes the view that learners should be educated about their safe use. We encourage lecturers to agree behavioural rules with their groups to maximise student success. These rules are likely to include non-use of social networking sites unless they are integral to the lesson content. Lecturers can then utilise the formal disciplinary procedures for persistent offenders.

In the LRC, users who are blocking the legitimate educational use of the IT equipment by using social networking sites will be asked to vacate the equipment. Bullying or

other inappropriate use of social networking sites is a disciplinary offence for staff and learners. IT Services will assist and advise in IT related disciplinary investigations.

7.4 Email

The use of email has the potential to allow access to the college system and therefore we use spam filtering system to minimise unwanted and offensive content. The Malicious Communications Act 1988 makes it an offence in England and Wales to send a message intending to cause distress or anxiety, whether this takes the form of threat, offensive material or false statements.

Learners and staff are made aware that the college reserves the right to gain access to any email document sent by them to recipients both inside and outside the college. Email usage rules are contained within the College's IT Conditions of Use Policy. Staff and learners are advised to not reveal personal details in email communications, such as date of birth, personal address or telephone numbers unless necessary.

7.5 Complaints regarding E–Safety

Complaints regarding general misuse of IT resources which disturb the learning opportunities of learners themselves or fellow learners should be managed by the classroom lecturer, as appropriate, using the relevant disciplinary procedures. Complaints regarding e-safety issues will be dealt with in accordance with the College's Safeguarding Procedures.

The DSL or Safeguarding Team will confidentially record all relevant details, including learner name, date of birth, address, allegation details, contact telephone numbers and any known family details. These details will be recorded on the safeguarding referral database by the Safeguarding Team.

The DSL will need to determine whether, in accordance with the Safeguarding Procedures, the allegation or suspicion of abuse requires any one of the following interventions:

1. Referral to a college mentor for additional support

2. Refer for an Early Help Assessment (EHA) – appropriate when a child or vulnerable adult is at risk of not meeting any one of the five Every Child Matters outcomes (Staying safe, Being healthy, Enjoy and achieve, Economic Wellbeing, Making a Positive Contribution) and the support of more than one publicly funded agency is required. This requires the consent of the child's parent/guardian, or the child him or herself if over 12 years of age, considered to be Gillick competent according to Fraser Guidelines and unable or unwilling to involve parents or guardians.

3. Referral to Children's Social Care (known as 'First Response' in Staffordshire) or the Police Child Protection Unit.

If the DSL is unsure of the most appropriate course of action to take, contact will be made to with a trained social worker by contacting Staffordshire's First Response child protection service, a Joint Assessment Coordinator or a Local Authority Designated Officer.

Any allegations of abuse against a staff member must be reported immediately to the DSL who will refer the matter to the LADO. They will advise the college on the procedural steps to be followed.

8.0 Legislation underpinning the Policy

8.1 This policy will be implemented in accordance with all existing and emerging legislation, including:

- The Children Act 1989
- The Protection of Children Act 1999
- School Education Act 2002 (Section 175)
- DfEE Circular 10/95 (Protecting Children from Abuse: The Role of the Education Service)
- Working Together to Safeguard Children

9.0 Monitoring and Review

9.1 This policy will be reviewed by the Board of Governors every two years.

9.2 The internal monitoring of the implementation of this policy will be the responsibility of the Assistant Principal – Learner Services, who will produce an annual Safeguarding report for the Board of Governors, which will include information and analysis on e-safety issues.