SOUTH ESSEX COLLEGES GROUP

E-SAFETY POLICY

2025-28

SIGNIFICANT CHANGES FOLLOWING REVIEW

PAGE NUMBER OR HEADING NAME	DETAILS OF SIGNIFICANT CHANGE	CHANGES MADE BY
All Document	Policy was updated following OU CMA feedback.	Head of Information Technology
Related Policies and Legislation (Page. 5)	New section	Head of Safeguarding
Definitions (Page. 5)	Updated to include the 4C's of e-safety as cited in KCSIE	Head of Safeguarding
Responsibilities (Page. 6)	Job titles and responsibilities updated	Head of Safeguarding
Security, Filtering & Monitoring (Page. 7)	Section updated to include information on filtering and monitoring. Inclusion of the use of generative AI	Head of Safeguarding
Uses of Images (Page. 8)	Reference to Appendices B & C	Head of Safeguarding
Education & Training (Page 9)	Updated to reflect current practice	Head of Safeguarding
Incidents & Response (Page. 11)	Job titles and flowchart updated to reflect current practice	Head of Safeguarding
Appendix B (Page. 14)	Contact information added for the Safeguarding Team and external support agencies	Head of Safeguarding

Contents

E-Safety Policy

Introduction:

South Essex Colleges Group recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all students and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the College while supporting staff and students to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard students, we will do all that we can to make our students and staff stay safe online and to satisfy our wider duty of care.

Scope:

The policy applies to all students and staff and all members of the College community who have access to the College IT systems, both on the premises and remotely. Any user of College IT systems must adhere to and accept the Acceptable Use Agreement. The e-Safety Policy applies to all use of the internet and forms of electronic communication including email, mobile phones, social media, instant messaging, webinar platforms, video conferencing software (e.g. Teams, Zoom), and online collaboration tools.

Related Policies & Legislation

• Safeguarding Policy & Procedure • Supporting Positive Behaviours Policy & Procedure (FE) • Higher Education Disciplinary Policy • Student Anti-Bullying Policy • Freedom of Expression Policy • Staff Disciplinary Policy • Information Security Management Policy • Acceptable Telecommunications, Network & Internet Use Policy • Computing Services Terms of Use • Use of AI Policy • Bring Your Own Device Policy	• Online Safety Act 2023 • Keeping Children Safe in Education (KCSIE) • Education Act 2002 • Children Act 1989 & 2004 • Data Protection Act 2018 (UK GDPR) • Prevent Duty (Counter Terrorism and Security Act 2015) • Malicious Communications Act 1988 & Communications Act 2003 *See Appendix F for further information on the relevant UK Legislation and guidance*

Definitions:

The term e-safety is defined for the purposes of this document as the process of limiting the risks to children, young people and vulnerable adults when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and inspection.

E-safety risks can be summarised under the following four headings:

Content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes. Use of Spyware, e.g. use of Remote Access Trojans/Tools to access private information or spy on their victim.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Adapted from: Keeping children safe in education - GOV.UK

Responsibilities

The Head of Information Technology and Head of Safeguarding are responsible for maintaining this policy.

The following are responsible for implementing it:

- The Head of Safeguarding is responsible for keeping up to date with new technologies and their use, as well as attending relevant training. They will deliver staff development and training, record incidents, report any developments and incidents and liaise with the local authority and external agencies to promote e-safety within the College community.
- The Safeguarding Team will provide pastoral and practical support for students dealing with issues related to e-safety.

- The Department of Human Resources for all e-safety matters in relation to College staff.
- The Head of Information Technology is responsible for championing good e-safety practice in College IT facilities and processes, and for providing technical expertise when issues are being investigated. The Head of Information Technology will also maintain the Colleges Group Cyber Essentials accreditation.
- The Student Experience SLT Lead ensuring that eSafety has a place in the central tutorial programme.
- All tutors for embedding e-safety education and practice into their teaching programme, and managing online behaviour concerns as they arise.
- All College Managers for implementing good e-safety practice and safeguards consistent with this policy in their area of responsibility.
- All members of College staff for staying alert to and responding appropriately to any potential or actual e-safety issue.

Security, Filtering & Monitoring

The College will do all that it can to make sure the College network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, workstations to prevent accidental or malicious access of College systems and information. Digital communications, including email and internet postings, over the College network, will be monitored in line with the Acceptable Use Policy.

The College will ensure there are appropriate filters and monitoring systems in place and regularly review their effectiveness so we can reasonably limit the exposure to online risks whilst balancing the need for open education which is age and level

appropriate. The College will comply with the DfE's Filtering and Monitoring Standards.

The College complies with guidelines set out by the Counter Terrorism Internet Referral Unit (CTIRU) and has a statutory duty to ensure their systems cannot be used to access any of the websites on the CTIRU list.

The College will consider the risks and challenges alongside the opportunities and benefits of generative AI as research and evidence emerges. More guidance on the safe use of AI can be found in Appendix F.

Behaviour

South Essex College Group will ensure that all users of technologies adhere to the standard of behaviour as set out in the Acceptable Use Policy.

The College will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and students should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student behaviour and staff disciplinary procedures.

Use of Images and Video

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or students.

All students and staff should receive training on the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted onto social networking sites, for example. Further information is available in Appendix B and C.

South Essex Colleges Group teaching staff will provide information to students on the appropriate use of images as detailed in the Acceptable Use Policy. This includes photographs of students and staff as well as using third party images. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

No image/photograph can be copied, downloaded, shared or distributed online without permission from the owner. Photographs of activities on the College premises should be considered carefully and have the consent of the Marketing department before being published. Approved photographs should not include names of individuals without consent.

Education and Training

With the current unlimited nature of internet access, it is impossible for the College to eliminate all risks for staff and students. It is our view therefore, that the College should support staff and students to stay esafe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

For students:

Students on 14-16 and 16-18 programmes will have e-safety embedded through tutorial and curriculum sessions as well as the opportunity to attend eXtra+ enrichment sessions throughout the year. An area on the VLE has also been set up with e- safety resources which are signposted at induction. Students should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search. These modules and assessments are primarily formative, designed to raise awareness and build safe online behaviour skills.

Within classes, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

Students will be taught a range of digital literacy skills which will also include e-etiquette on the use of college systems such as Teams and Outlook.

Appendix A shows E-Safety Guidelines, Appendix B shows Guidelines for Students (Social Media) and Appendix D shows Guidelines for students using webinar / video conferencing software.

For staff:

Staff will take part in mandatory Safeguarding training with updates on online safety a minimum of every 3 years.

Staff will also be asked to sign the College (staff) Acceptable Use Policy. Appendix A shows E- Safety Guidelines, Appendix C shows Guidelines for Staff (Social Media) and Appendix E shows Guidelines for staff using webinar / video conferencing software.

Incidents and Response

The guidelines and flowchart below are to support any staff member dealing with an e-Safety incident

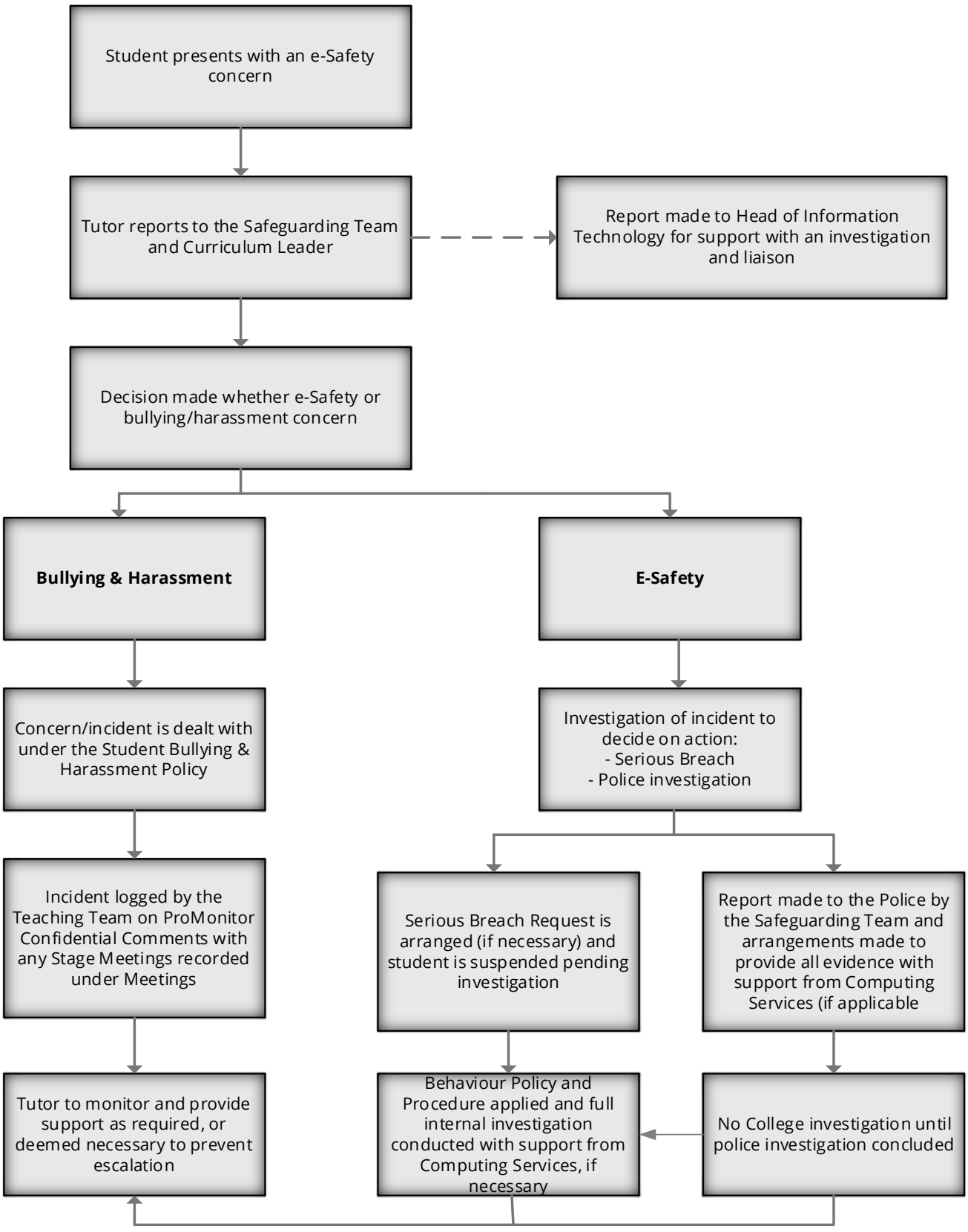
When it becomes apparent that a young or vulnerable person has been the victim of bullying or harm, including radicalisation, through online activity and technology, the following steps should be taken:

- Ensure the young or vulnerable person is safe and no longer at risk of harm
- Check that others are not at immediate risk of harm from the same e-Safety issue
- Contact the Safeguarding Team and Head of Information Technology.
- Cooperate with the Safeguarding Team, Computing Services or Police investigation as required.
- Talk to your line manager if you feel in need of support following exposure to the incident.
- Reflect on what you and other staff can learn from the experience to reduce such incidents in future. These lessons should be discussed in team meetings or reviews, integrated into updated training sessions, and shared via internal communications. Response to incidents should occur as soon as the issue is identified, ideally within 24 hours for safeguarding concerns and within 72 hours for lower-risk issues.
- e-Safety incidents will be dealt with under the Supporting Positive Behaviours and/or the Student Bullying & Harassment Policy or relevant HE policy.

Appropriate formal outcomes will be given after thorough investigation. It may be apparent to implement the Safeguarding Policy (including Prevent) if appropriate.

e-Safety incidents relating to Staff will be dealt with under the Disciplinary Policy and Procedures and referred to within the Staff Code of Professional Conduct.

E-Safety Incident Flowchart



Appendix A - E-Safety Guidelines

- Keep your personal information private – avoid sharing personal information such as your phone number, home address or photographs with people you don't know in person and trust.
- Check whether the social media networks you use allow you to create friend lists. These lists let you manage who sees what. For example, you may only want your closest friends to see some information.
- Use private messages for people you know in person and trust; be careful of private messaging people you don't know.
- Use a strong and unique password for all of your online accounts – a combination of letters, numbers and symbols
  (and if you've ever shared it in the past, CHANGE IT).
- Know how to block someone if they make you feel uncomfortable or upset.
- Learn how to save chat logs and texts so that if someone does make you uncomfortable or upset, you have evidence to report them.
- Remember to log out of a site properly after use, especially on a shared computer.
- Keep your clothes on when using webcam – images of you could end up in the wrong hands!
- Think very carefully about meeting someone face to face who you only know online – NEVER do this alone, always talk to your parents or carers before you go ahead with this and take a trusted adult friend along with you.
- Students or staff should report any abusive behaviour immediately to the Safeguarding Team s e e Appendix B – Guidelines for Students (Social Media) for further information

Appendix B: Student Guide for Social Media

As part of our duty of care to our students, the College sets out guidelines, below, for students when using social media.

- Students should follow the guidelines below at all times:
- Do not enter into a "friends" relationship online with someone you do not know
- Do not request to follow or "friend" a member of staff
- Do not use social media to harass, threaten, insult, defame or bully another person or entity; to violate any College policy; or to engage in any unlawful act, including but not limited to gambling, identity theft or other types of fraud
- Do not access or participate in social media which insights hatred or promotes radicalisation.
- Set up privacy settings carefully, ensure you are not sharing any information that you do not want to and check these on a regular basis
- Participating in social media use as part of a College or course activity is optional. Students may opt out at any time Students wishing to opt out should inform their tutor or course leader in writing or via email.
- Discussions on South Essex Colleges Group branded social media should be appropriate and College or Course related
- When posting on sites linked to South Essex Colleges Group or when mentioning or referring South Essex Colleges Group on social media do not:
    - Use foul or abusive language
    - Harass, threaten, insult, defame, blackmail or bully another person
    - Refer to any other member of the South Essex College Group community, whether student or staff, in a derogatory or insulting manner
    - Refer to the College, its courses or facilities or any other aspect of its offering, in a derogatory or insulting manner
    - Post or comment in any way that reflects poorly on the College or is deemed to interfere with the conduct of College Business
- Posting of messages that are deemed inappropriate will be dealt with under the student disciplinary procedure

- Copies of inappropriate posts may be reported to parents/guardians and the appropriate authorities. Before you post a message, think carefully about its content and ask yourself how you would feel if you received that message or know that it may be disclosed in court In cases involving students under the age of 18, parents or guardians may be contacted. For HE students, appropriate safeguarding procedures will apply instead.
- Any form of abuse or cyber-bullying will be dealt with under the student disciplinary procedure
- Students should report any abusive behaviour immediately to the Safeguarding Team:
    - Via Whisper Online Reporting: https://swgfl.org.uk/WHISPER/SEC1/
    - Via Email: Safeguarding@Southessex.ac.uk
    - In person at the safeguarding Offices at every campus
    - Via their tutor or any member of staff
- Where a student or staff member comes across harmful content online they are able to flag this with Computing Services and/or the Safeguarding Team. Reports can also be made to Report Harmful Content and more information on community guidelines of apps/site scan be found here
    - Report Harmful Content - We Help You Remove Content
- If image based sexual abuse is reported this must be reported to the Safeguarding Team. Further advice and guidance can be found here:
    - Under 18's: Report Remove | Childline
    - https://revengepornhelpline.org.uk/how-can-we-help/how-to-get-in-touch/

Appendix C – Guidelines for Staff (Social Media)

This policy sets out guidelines for staff, below, for the use of social media.

These guidelines apply to:

- Posting to any South Essex College Group social media site;
- communicating with members of the South Essex College Group community including staff or students;
- discussing the College on any site;

Whether at College and using the College network and equipment or through a personal account or using a personal phone, computer or other device from any other location.

Staff should follow the guidelines below at all times:

- Be professional; as a South Essex College employee you are an ambassador for the organisation. Protect the South Essex College brand and values at all times, do not make derogatory comments about South Essex College Group products, services, management, employees or systems
- Never have a "friend" relationship with a student online, where personal details are shared
- If the Social Media requires a login, create a separate "work" login and ensure any privacy settings are set appropriately so that no personal information can be viewed.
- Staff should not share any personal information online including home address, personal telephone numbers, personal email addresses or date of birth
- Discussions on social media sites linked to South Essex Colleges Group should be appropriate and be College or Course related

  When using Facebook (in line with the Social Media Reputational Management Policy), Pages are permitted and monitored by the Marketing department. Groups are not permitted, online discussion and communication should take place on College systems (e.g. Cloud) which are closely monitored.
- When communicating with students who are under 18 via email, College

student email addresses should be used.

- Email communications with students under 18 must happen within normal working hours (8.30 – 5pm).
- Staff should not comment on anything related to legal matters, litigation, or any parties the College may be in dispute with or anything that may be considered a crisis situation.
- Do not access or participate in social media which insights hatred or promotes radicalisation.
- Do not upload to video/photo sharing sites (e.g. YouTube) unless it is done via the South Essex Colleges Group official channel. Contact Marketing to do this
- Do not post a person's photograph or video image without first obtaining permission and signed release forms from anyone depicted in the photograph or video (any photographs of children and young people under the age of 16 should have parental permission) Blank release forms may be requested from the Marketing team and should be promptly returned after they are signed
- Protect confidential and sensitive information at all times (e.g. referring to sickness absence of others etc.)
- Whenever appropriate, link back to information posted on the College website instead of duplicating content. For assistance with linking to the website please contact the Marketing team
- Remember that statutory regulations and South Essex Colleges Group policies including inappropriate conduct such as sexual (or other) harassment, bullying, discrimination, defamation, infringement of copyright and trademark rights, data protection and unauthorised disclosure of student records and other confidential and private information, will apply to communications by South Essex Colleges Group students and staff through social media
- When posting on sites linked to South Essex Colleges Group or when mentioning or referring to South Essex Colleges Group on social media do not:

  - Use foul or abusive language
  - Harass, threaten, insult, defame or bully another person
  - Refer to any other member of the South Essex Colleges community, whether student or staff, in a derogatory or insulting manner

- Refer to the College, its courses or facilities or any other aspect of its offering, in a derogatory or insulting manner
- Post or comment in any way that reflects poorly on the College or is deemed to interfere with the conduct of College business

- Staff should not spend an excessive amount of time while at work using social media websites in a personal capacity. They should ensure that use of social media does not interfere with their other duties as this is likely to have a detrimental effect on productivity
- Any breach in this Policy could result in an investigation and disciplinary procedures under the staff disciplinary policy. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing reputational damage to the College, may constitute gross misconduct and lead to dismissal.
- Staff should abide by the Guidelines on Professional Boundaries and Standards.

Appendix D – Guidelines for students using webinar / video conferencing software

This policy sets out guidelines for students using webinar/video conferencing software:

Do:

- Conduct yourself in a professional manner throughout calls with tutors, support staff or other students.
- Attend video calls from a desk or other appropriate location. If you do work from your bedroom, you MUST blur your background.
- Make sure you are dressed appropriately
- Be punctual and courteous. Language must be professional and appropriate. Turn your phone to silent. Treat this just like you would a lesson or meeting at College.
- Look at your screen, pay attention to others and when speaking make sure to look at your camera.
- Use the 'blur background option' to hide any background if needed.
- Check what you can see when you first log in as this is what others will see.
- Mute your microphone when not needing to talk to avoid any background noise.
- Position yourself away from where your family members or pets are.
- Only post chat messages relevant to the lessons

Don't:

- Conduct/attend a video call if it would be improper for a face-to-face meeting.
- Multi-task; the tutor will be aware.
- Shout; the other participants will tell you if they cannot hear.
- engage in behaviours that may distract others unless these are needed for neurodiverse coping (e.g., stimming). In such cases, students are encouraged to discuss reasonable adjustments with their tutor..
- Eat or drink, other than water / tea / coffee
- Leave multiple applications open during the call as it may affect the quality.

Appendix E – Guidelines for staff using webinar / video conferencing software

This policy sets out guidelines for staff using webinar/video conferencing software:

Do:

- All 1:1 online activity with under 18s or vulnerable adults MUST be agreed with students prior to the 1:1 taking place. The 1:1 must then take place only at the days / times agreed.
- If at any time you feel uncomfortable during a 1:1 call, with something done or said, you should end the call as soon as possible and report any concerns to your line manager and / or safeguarding. Examples may include: student inappropriately dressed or in an inappropriate location (eg bedroom).
- Please note: If your safeguarding training is not up to date you MUST NOT conduct a 1:1 video conferencing session. Refer to your line manager for further guidance.
- Where possible set up online meetings/lessons with students through teams channel and use the waiting rooms facility. This prevents unwanted guests and avoids 'Zoom Bombing'.
- Encourage students to maintain an awareness of employability skills in how they conduct themselves in online sessions.
- Conduct yourself in a professional manner throughout calls with colleagues or students - you remain an employee of South Essex College Group throughout the call.
- Conduct video calls to students or colleagues from a desk or other appropriate location. If you do work from your bedroom, you MUST blur your background.
    - Remind students that all calls/videos may be recorded - this is to safeguard both parties and wouldn't routinely be shared.
    - Be punctual and courteous. Language must be professional and appropriate. Introduce yourself and take note of other attendees' so you can address them by name. Turn your phone to silent. Treat this just like you would a face to face meeting with a student, colleague or other adult.

- Test your audio and/or video before a scheduled call.
- Look at your screen, pay attention to others and when speaking make sure to look at your camera.
- Use the 'blur background option' to hide any background if needed.
- Check what you can see when you first log in as this is what others will see.
- Mute your microphone when not needing to talk to avoid any background noise.
- Position yourself away from where your children, spouse, or pets are.

Don't:

- Conduct a video call if it would be improper for a face-to-face meeting.
- Multi-task; your audience will be aware.
- Shout; the other participants will tell you if they cannot hear.
- engage in behaviours that may distract others unless these are needed for neurodiverse coping (e.g., stimming). In such cases, students are encouraged to discuss reasonable adjustments with their tutor..
- Eat or drink, other than water / tea / coffee
- Leave multiple applications open during the call as it may affect the quality.
- Wear stripes or heavy patterns creating pixilation of images.

Appendix F: Legislation Overview

Below is a list of key UK legislation and statutory guidance relevant to **e-safety in education**:

📘 **1. Online Safety Act 2023**

- **Purpose**: Introduces legal duties for online platforms to protect users, especially children, from harmful content.
- **Key Provisions**:
  - Platforms must assess and mitigate risks to children.
  - Stronger age verification and content moderation.
  - Ofcom is the regulator enforcing compliance [1] [2] [3].
- **Relevance to education**: While the Act targets tech companies, institutions must understand its implications for digital literacy and safeguarding education.

📗 **2. Keeping Children Safe in Education (KCSIE)**

- **Statutory guidance** for schools and colleges in England.
- **Includes**:
  - Requirements for filtering and monitoring online activity.
  - Staff training on online risks (e.g., cyberbullying, grooming).
  - Policies for reporting and managing online safety concerns [4].

📙 **3. Education Act 2002**

- **Section 175** places a duty on education institutions to safeguard and promote the welfare of children, which includes online safety.

📕 **4. Children Act 1989 & 2004**

- Establishes the legal framework for child protection, including digital environments.

📒 **5. Data Protection Act 2018 (UK GDPR)**

- Governs how institutions handle children's personal data online.
- Includes rules on consent, especially for under-13s using online services.

📓 **6. Prevent Duty (Counter-Terrorism and Security Act 2015)**

- Requires education institutions (schools, FE & HE) to protect pupils from radicalisation, including through online content.

📘 **7. Malicious Communications Act 1988 & Communications Act 2003**

- Addresses cyberbullying, online harassment, and harmful communications.

📜 Additional Guidance

- **NSPCC Online Safety for Schools**: Offers practical advice on e-safety policies, training, and parental engagement [5].
- **Teaching Online Safety in Schools** (DfE): Curriculum guidance (Up to KS4) for digital literacy and resilience [3].
- **Using AI in education settings** (DfE): Support materials to help schools and colleges use AI safely and effectively. Free support materials for staff and for leaders. [6]

References

[1] What the Online Safety Act means for children | Internet Matters
[2] Online Safety Act 2023 - Legislation.gov.uk
[3] What is the Online Safety Act and what does this mean for ... - Brachers
[4] Keeping children safe in education - GOV.UK
[5] Online safety (e-safety) and schools | NSPCC Learning
[6] Using AI in education settings: support materials - GOV.UK

Appendix G: Equality Impact Assessment

The aim of an equality impact assessment (EIA) is to consider the equality implications of any new or amended policy, procedure, practice, project, function on different groups of staff, students and visitors to the college. This EIA tool provides a simple framework that helps evaluate whether the change may inadvertently disadvantage protected characteristics and identify ways to proactively advance and promote equality.

You will need to consider each of the equations and provide information as to consideration and any changes made in relation to Equality, diversity and inclusion.

Date EIA completed.	June 2025
Name of person responsible for completing the EIA	Jane Belcher
Role of person responsible for completing the EIA	Interim Director of ALS, Safeguarding & Learner Wellbeing
Who is affected by the policy / decision / change	All staff and students
What's the reason for the new policy / change in policy, practice, process etc.	Updates are in line with legislation and statutory guidance on safeguarding

You will need to consider whether it's possible that the proposed new policy / change in policy /procedure/practice etc could discriminate or unfairly discriminate or disadvantage people. You should consider:

Who gets to participate	Who does not, or who now does not due to the changes proposed / made.
Who is at an advantage	Who is at a disadvantage, and again has this changed?
Who will benefit	Who will not benefit (or who did and now doesn't due to the changes proposed in policy
Who can access the policy	Who cannot, or now cannot.

What are the overall aims of the change? Why are you proposing it?	The aim of this policy is to provide a framework to ensure that the guidelines are in place to support all stakeholders
Given the aims of your proposal, what issues does your data/information highlight?	Everybody is included within this policy, and all groups are given equability in regards to their needs and provisions
How could the proposed change affect positively/negatively	This has a positive impact on all groups with protected

on groups with protected characteristics?	characteristics, as they are ensured equal treatment and provision based on their needs. Risk assessments may be carried out to ensure that this is the case and provisions maybe altered to accommodate specific needs
What actions will you take to mitigate any negative impact?	No negative impact to having this policy
Is there any potential negative impact justified in light of wider benefits of the proposal	No negative impact to having this policy
Recording final decision	This policy requires Executive approval

Has the policy taken into consideration the requirements of GDPR regulations? Are there any actions that need addressing, e.g.; data sharing agreement; has data consent been considered; data retention	GDPR regulations have been considered and actions comply with data protection requirements.

Protected Characteristic	What degree of impact does the change have (score 1-5 with 1 the lowest and 5 the highest)	What is a potential positive, neutral or negative impact? Include what you have considered. Are there any barriers?	What action will be taken to address any negative impact or remove any potential barriers identified? Note if we are not able to resolve anything identified.	Date by when and whom will this action be taken.
Age	1	None identified		
Disability	1	Some potential barriers to accessing/reading and understanding documentation	Appropriate action will be taken to ensure any person who discloses a health concern and/or disability are provided with adjustments to enable them to understand and be aware of processes	As and when required
Gender (Sex)	1	None identified		
Gender Reassignment	1	None identified		
Marriage or Civil Partnership	1	None identified		
Pregnancy / Maternity	1	None identified		
Race	1	None identified		
Religion or Religious Belief	1	None identified		
Sexual Orientation	1	None identified		
Any other element that needs to be considered.	1	Persons where English is not a first language	Appropriate action will be taken to ensure any person who discloses English as a second language are provided with adjustments to enable them to understand and be aware of processes	As and when required

Note:

1. The terms stated under protected characteristics are the terminology used in the Equality Act 2010.

As part of the policy approval process Executive Board will consider the EIA assessment and any potential barriers which we may not be able to overcome and whether the action proposed will mitigate sufficiently within legislation or whether we decide to not implement the new policy if the risk are significant. If the policy is approved the EIA is also approve

Senior Leadership Responsibility	Interim Director of ALS, Safeguarding & Learner Wellbeing
Policy Author	Interim Director of ALS, Safeguarding & Learner Wellbeing
Roles Responsible for Reviewing	Interim Director of ALS, Safeguarding & Learner Wellbeing Safeguarding Manager Head of Information Technology Learning Technology Manager
Issue date of current version	June 2025
Date to be reviewed	June 2028
Type of Policy	Public