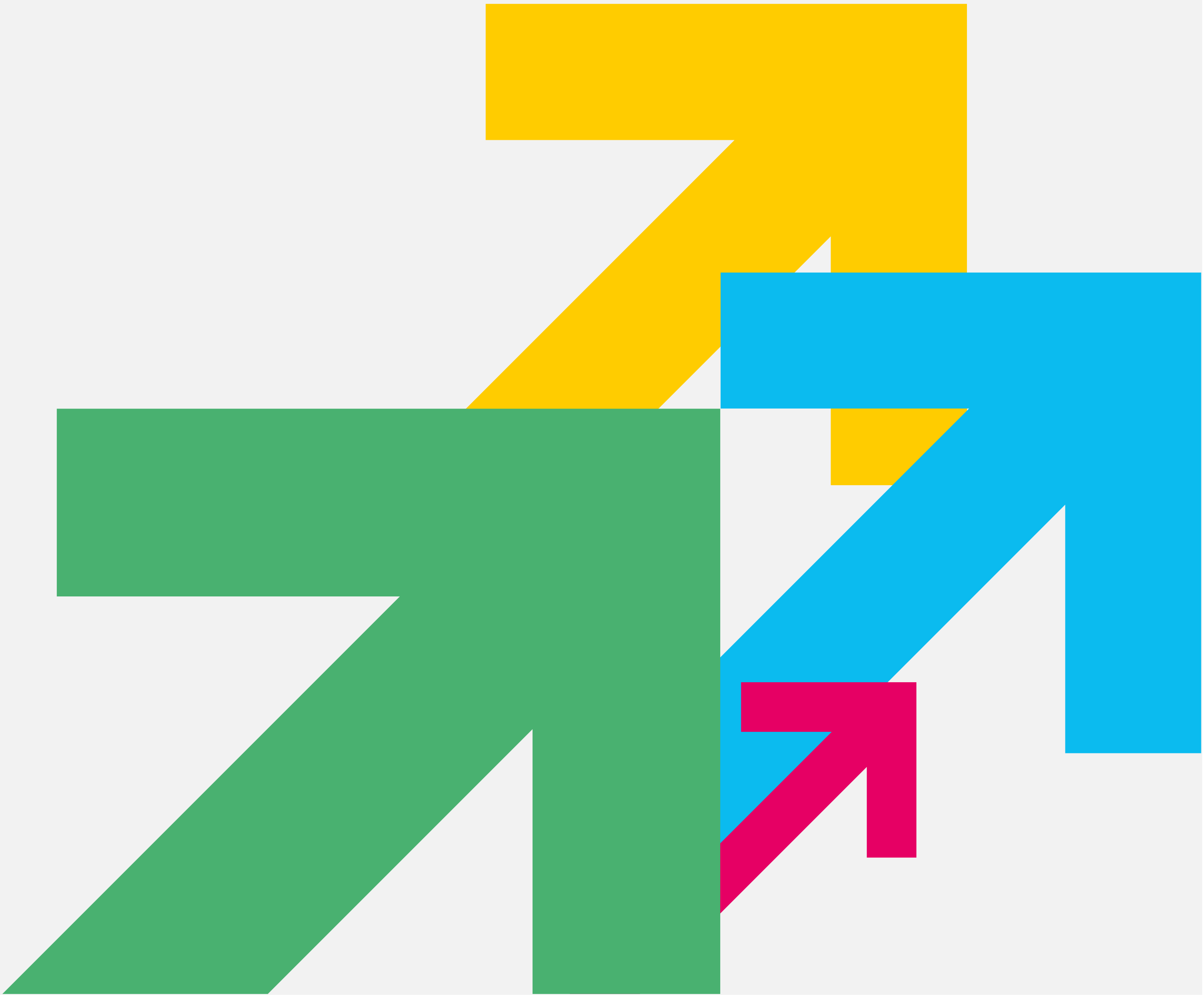
South Thames Colleges Group

e-Safety Policy

July 2023

RAD Volo



E-SAFETY POLICY

Purpose
The Colleges Group recognise 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 Group 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 sure our students and staff stay safe online and to satisfy our wider duty of care.

Scope
The policy applies to all students and staff who have access to the Group IT systems, both on the premises and remotely. This e-Safety Policy applies in all use of the internet and forms of electronic communication such as email, mobile phones, social media, instant messaging etc.

Definition
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 through a combined approach of policies and procedures, infrastructures and education (including training), underpinned by standards and inspection.

e-Safety risks can be summarised under the following three headings.

Content
- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance, sites promoting radicalisation or pornography
- Exposure to illegal material, such as images of child abuse
- Illegal Downloading of copyrighted materials e.g. music and films

Contact
- Grooming using communication technologies, potentially leading to sexual assault, child sexual exploitation and radicalisation
- The use of assumed identities on gaming platforms
- Bullying via websites, mobile phones or other forms of communication device
- Spyware, e.g. use of Remote Access Trojans/Tools to access private information or spy on their victim

Commerce
- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

Security
The Colleges Group will do all that it can to make sure the Groups networks are 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 and work stations to prevent accidental or malicious access of Group systems and information. Digital communications, including email and internet postings, over the Group networks, will be monitored in line with this Policy.

General 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 each 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.

Specific e-Safety Guidelines for staff

1. Be professional; as a College employee you are an ambassador for the organisation. Protect the College brand and values at all times; do not make derogatory comments about College products, services, management, employees or systems.
2. Never have a "friend" relationship with a student online, where personal details are shared.
3. 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.
4. Staff should not share any personal information online including home address, personal telephone numbers, personal email addresses or date of birth.
5. Discussions on social media sites linked to the College should be appropriate and be College or Course related.
6. 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.
7. Do not access or participate in social media which insights hatred or promotes radicalisation.
8. Do not upload to video/photo sharing sites (e.g. YouTube) unless it is done via the College official channel.
9. 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).
10. Protect confidential and sensitive information at all times (e.g. referring to sickness absence of others etc.)
11. Whenever appropriate, link back to information posted on the College website instead of duplicating content.
12. Remember that statutory regulations and College 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 College students and staff through social media.

13. When posting on sites linked to the College or when mentioning or referring to College 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 College 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.

14. 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.
15. 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.

Specific e-Safety Guidelines for students

1. Do not enter into a “friends” relationship online with someone you do not know.
2. 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.
3. Do not access or participate in social media which insights hatred or promotes radicalisation.
4. 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.
5. Participating in social media use as part of a College or course activity is optional. Students may opt out at any time.
6. Discussions on College branded social media should be appropriate and College or Course related.
7. When posting on sites linked to the College or when mentioning or referring to the College 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 College 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.
8. Posting of messages that are deemed inappropriate will be dealt with under the student disciplinary procedure.
9. 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.
10. Any form of abuse or cyber-bullying will be dealt with under the student disciplinary procedure.