Policy Name:	E-Safety Policy
Policy Number/Version No:	
Effective Date:	February 2022
Review Date:	May 2023
Policy Responsibility:	Vice-Principal, Finance and Planning / IT Manager
Approved By:	SLT
For Action By:	All College staff, students, Governors, volunteers and contractors
For Information to:	All College staff, students, parents/carers, Governors, volunteers and contractors

1 Introduction

1.1 Richmond Upon Thames College is dedicated to promoting our values of honesty, integrity, mutual respect and personal accountability to support our students in becoming fully rounded members of society with a strong sense of social and moral responsibility. We prepare our students for life in Modern Britain by developing an understanding of democracy, the rule of law, individual liberty, mutual respect and tolerance of those with different faiths and beliefs and this is reflected in our policies.

1.2 The College recognises the benefits and opportunities which new technologies offer to teaching and learning and to all our students. We encourage the use of technology not only to enhance students' learning experience but also to promote skills and achievement. However, the accessible and global nature of the internet and associated technologies means that we are also aware of the potential risks faced, such as privacy invasion, grooming, cybercrime, cyber-bullying, commercial exploitation, child criminal exploitation, radicalisation and educational misconduct and the challenges involved from these.

Our approach is to implement safeguards within the college which will support staff and students to manage any potential risks and to deal with these risks independently. We believe that this can be achieved through a combination of security measures, training, guidance and implementation of our associated policies. In furtherance of our duty to safeguard learners, we will do all that we can to make our learners and staff stay 'e-safe' and to satisfy our wider duty of care in accordance with *Keeping Children safe in Education* (DfE, 2021) ("KCSIE")

The statutory responsibilities associated with online safety include the need for all staff to be aware of the role of technology within:

- sexual and emotional abuse
- Child Sexual Exploitation
- radicalisation

Staff also need to be aware that abuse can be perpetrated by children themselves and guidance specifically identifies sexting and cyberbullying.

2 Scope

2.1 This policy applies to all students, both prospective and current, and staff. The technologies encompassed within this policy include all computer-based technologies, online communication technologies, digital technologies both fixed and mobile. This includes use of the internet, e-mail, mobile phones, games consoles, social networking sites and any other systems that use the internet for connections and providing information. This would include use of both College owned and non-college owned devices as outlined in the RuTC Bring Your Own Device Policy.

2.2 The Education and Inspections Act 2006 empowers Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the College site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the College but is linked to membership of the College. Richmond upon Thames College will deal with such incidents within this policy and associated behaviour and anti-bullying policies and

will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of college, where the student is under aged 18.

Safeguarding (including online safety) is the responsibility of everybody who works within the College.

The KCSIE document identifies that education settings are responsible for ensuring that:

- appropriate filtering and monitoring of internet access is in place
- all members of staff receive appropriate training and guidance
- the curriculum preparing children and young people for the digital world.

The Principal (Senior Designated Safeguarding Lead) and Head of Student Experience are part of the Technology Strategy group who keeps up to date with new digital technologies and platforms and will provide input on e-Safety. In the event of safeguarding issues arising the Safeguarding Policy should be followed.

This E-Safety Policy should be read in conjunction with other relevant policies, in particular the college Computer Network, Internet and Intranet Acceptable Use Policy for computer equipment, the Social Media Guidelines (Appendix B), Safeguarding Policy, the Anti-Bullying Policy, the Student Support and Disciplinary Policy and the Student Code of Conduct.

3.0 Objectives

3.1 To ensure safeguards on college IT-based systems are strong and reliable and students know how to report issues.
3.2 To ensure user behaviour is safe and appropriate.
3.3 To ensure that student storage and use of images and personal information on college IT- based systems is secure and meets all legal requirements.
3.4 To educate Students in e-safety.
3.5 To ensure any incidents which threaten e-safety are appropriately reported and managed effectively.

4.0 Security

- students will be provided with a username and a strong password (minimum 14 characters) and will be required to use MFA (Multi Factor Authentication). Students should help keep networks secure by ensuring that their log-in details are kept private and not shared with anyone else.
- students will have clearly defined access rights to college technical systems and devices and should not breach these.
- students are aware that digital communications, including email and internet postings, over the college network are effectively monitored by college technical and safeguarding staff and records of the activity of users logged.
- students are aware that internet filters are used to minimise access to inappropriate websites.
- students are aware that computer monitoring is in use by staff, both in the LRC and in many classrooms, as outlined in the Student LRC/IT Induction at the beginning of the year.
- students are aware of procedures to report inappropriate or illegal content, including use of the CEOP reporting system.

- students are aware that they are required to secure their devices and update them.
- risk assessments carried out when learners are off-site are to include e-safety.
- All college devices are updated and patched on a regular basis.
- students should have a lock (biometric and password) on their personal devices. Students are asked to create strong passwords for online accounts and to be different to their college account.
- students should follow the Online Learning Platform Policy and Guidelines for any remote learning activity.
-

5.0 Education

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. Education in online safety / digital literacy is therefore an essential part of the College's online safety provision. Young people need the help and support of the college to recognise and avoid e-safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum and in tutorials.
The DfE guidance document Teaching Online Safety in Schools provides guidance to staff on how to discuss e-safety principles with students, as well as guidance on types of risk in the digital space.

- Key online safety messages should be reinforced as part of a planned programme of induction/tutorial / pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside College.
- Learners 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.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

- Students will receive instructions and tutorial sessions on digital footprint.

6.0 Behaviour

6.1 All student users of technology are responsible for:

- adhering to the standards of behaviour set out in the Computer Network, Internet and Intranet Acceptable Use Policy.
- adhering to college guidance when using email, mobile phones, social networking sites, games consoles, chat rooms, video conferencing and web cameras etc.
- having a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- understanding the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the College's e-Safety Policy covers their actions out of school, if related to their membership of the school.

6.2 The college will not tolerate any abuse of ICT systems or associated technologies. Whether offline or online, communications by students should be courteous and respectful at all times. Any reported incident of bullying, harassment or other unacceptable behaviour will be treated seriously as set out in the Anti-Bullying Policy and Student Support and Disciplinary Policy.

Staff should be aware of the Colleges responsibility of the Prevent Duty and Safeguarding of young people and adults at risk. Where conduct is found to be inappropriate, the college will deal with this internally. Where conduct is considered illegal (it breaches the law e.g., copyright, extremism, abuse), the matter will be referred to the Police. Additionally, the college may seek to involve other agencies where conduct is believed to be unacceptable or illegal, or where it presents a safeguarding risk. Examples of behaviour that may lead to action are given below.

- Deliberately accessing or trying to access material that could be considered illegal (including extremist content)
- Taking images or videos of other members of the college community without their explicit consent (this includes students, staff, visitors, volunteers, contractors etc)
- Unauthorised use of non-educational sites during lessons
- Unauthorised / inappropriate use of mobile phone / digital camera /other mobile device
- Unauthorised / inappropriate use of social media / messaging apps / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access college networks by sharing username and passwords
- Attempting to access or accessing the college network, using another student's account
- Attempting to access or accessing the college network, using the account of a member of staff
- Corrupting or destroying the data of other users
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature including (but not limited to): use of sexually explicit language or viewing, creation or

sharing of sexually explicit imagery; verbally abusive, intolerant or threatening language; use of racist or extremist language which would directly contravene British values; use of social media for radicalisation or the expression of extremist views.

- Continued infringements of the above, following previous warnings or sanctions
- Actions which could bring the college into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the college filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act or General Data Protection Regulations

The above examples are not exhaustive or exclusive.

6.3 Any abuse of IT systems and any issues of bullying or harassment (cyber bullying) are robustly dealt with, in line with student disciplinary procedures.

Any conduct considered illegal is reported to the police.

7.0 Actions and Responsibilities

7.1 There are clear guidelines and lines of responsibility for online safety within the college.
All staff are responsible for ensuring the safety of students and should report any concerns immediately to their line managers whose first point of contact should be the Safeguarding Team. (Flow chart Appendix A).

The Learning Technologist delivers a session on the use of College systems during induction, including e-safety.

Each Curriculum area team is expected to arrange for students to be made aware of this policy and the ethos of online safety.

It will also be shared via the staff and student intranet and the website.

7.2 In line with the college Safeguarding Policy, staff should take care not to guarantee any measure of confidentiality to any individual reporting any concerns regarding online safety.

7.3 All students must know who to contact if they have any concerns regarding online safety. This includes the LRC staff, their tutor, the Designated Safeguarding Leads and/or relevant external agencies. They will be made aware of this via tutorials, the intranet and posters within the college

- If a student wishes to report an online safety incident, they can do so to any member of staff. The member of staff receiving the report will take appropriate immediate action to prevent any harm and record sufficient details to report the matter to the Safeguarding Team following the College's Safeguarding Procedures.

- Students will also be made aware of other reporting systems such as the CEOP link.

- Observations and concerns from staff members with regards to online safety incidents (i.e., a student accessing material which may pose potential harm) should be reported to the Safeguarding Team following the College's Safeguarding procedures.

- Reports via the College's IT monitoring and filter systems or breaches of the Computer Network, Internet and Intranet Acceptable Use Policy are likely to come to the attention of the IT Support Unit in the first instance. IT Support will then refer the matter to the Student Services Manager and/or the Safeguarding Team as appropriate.

- Concerns regarding online safety incidents involving members of staff should be reported to the Principal or Assistant Principal for Human Resources and Operational development.

8 Links to Other Policies

Safeguarding Policy

Anti-Bullying Policy

Student Support and Disciplinary Policy

Prevent Action Plan

RuTC Computer Network, Internet and Intranet Acceptable Use Policy

RuTC Bring Your Own Device Policy

Data Protection Policy

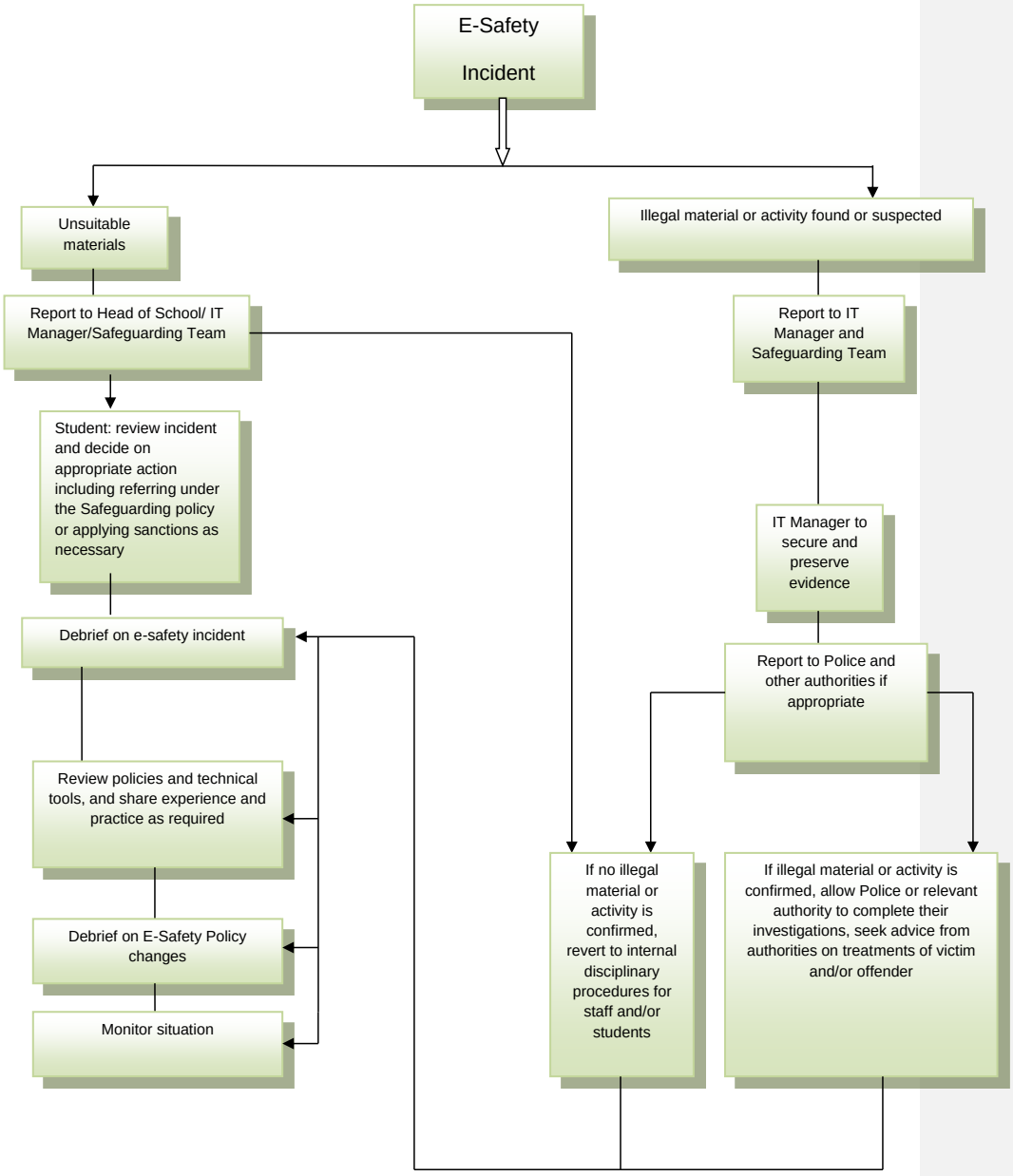
General Data Protection Regulations

Appendix A

Flowchart for responding to e-safety incidents

Commented [IR1]: Flowchart seems awry on my copy online?

Commented [IR2R1]: But seems OK in Word proper



Appendix B

Social Media Guidelines

1.0 Introduction

1.1 The College recognises the legitimate role and numerous benefits and opportunities that social media offers to the education and progress of students. Students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. The College is committed to maintaining confidentiality and professionalism at all times whilst also upholding its reputation so has an expectation that students using social media will exhibit appropriate conduct in ways that are consistent with college values and policies. These guidelines aim to encourage the safe use of social media by students.

1.2 Social media is a term used to describe the online tools, websites and interactive media that enable users to share information, opinions, knowledge and interests. Social media involves building online communities or networks, which encourage participation, dialogue and comment. Social networking applications include, but are not limited to blogs, online discussion forums, social and business networking, wikis, social bookmarking and tagging, photo and video sharing, and games that create virtual worlds, such as Fortnite and World of Warcraft. Examples of popular social media platforms include Facebook, Twitter, LinkedIn, Tik Tok, Instagram, WhatsApp, and YouTube.

2.0 Scope

2.1 These guidelines apply to all social media applications, including those currently in existence and any new platforms that may appear in the future. They also apply to any collaborative public information sites such as Wikipedia.

2.2 These guidelines apply to all students of the college, who are bound by the college Computer Network Internet and Intranet Acceptable Use Policy in relation to their use of social media and are particularly reminded of the College's commitment to equal opportunities and combatting bullying, including cyberbullying.

2.3 The College respects privacy and understands that students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the college's reputation are within the scope of these guidelines.

2.4 Professional communications are those made through official channels, posted on a college account or using the college's name. All professional communications are within the scope of this policy.

2.5 Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the college or impacts on the college, it must be made clear that student is not communicating on behalf of the college, with an appropriate disclaimer. Such personal communications are within the scope of this policy.

2.6 Personal communications which do not refer to or impact upon the College are outside the scope of this policy.

2.7 Digital communications with other students are also considered.

3.0 Privacy Settings and Personal Information

3.1 Default privacy settings for some social media websites allow some information to be shared beyond an individual's contacts. In such situations, the user of the site is personally responsible for adjusting the privacy settings for the account. Students are strongly encouraged to review their access and privacy settings for any social media sites to control, restrict and guard against who can access the information on those sites in preparation for employment.

3.2 Even if privacy and security settings are utilised, students should be aware that anything posted on social media sites may be made public by onward transmission or a change in a particular platform's policy.

3.3 Social media offers the ability to share personal information rapidly and easily. Students will be made aware of the importance of setting and protecting secure passwords and restricting personal information to reduce the risks of abuses such as identity theft through the curriculum and tutorials

4.0 Use of social media whilst at college

4.0.1 The College accepts that students may wish to use social media channels as a way of communicating personally with the public and friends about activities undertaken at the College. When sharing content pertaining to the College express permission should be obtained from Marketing or the relevant Curriculum Teacher and any other students involved in the post.

4.0.2 Students may wish to use their own personal devices, such as laptops, tablets, and smart phones, to access social media websites while at college. Students should be aware that the terms of the eSafety policy extend to this type of personal use.

4.0.3 Personal use of social media should not be used or interfere a with student's lessons. Excessive personal use or a failure to adhere to this policy may result in disciplinary proceedings.

4.1 College-related use of social media

4.1.1 Students are permitted to make reasonable and appropriate use of social media websites during lesson when directed to by a teacher as part of the learning activities, or as a particular project.
4.1.2 Permission to use any photos or video recordings should be sought in line with the College's guidelines on the use of digital and video images. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
4.1.3 Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
4.1.4 Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality

4.2 Contributing to College Social Media Channels

4.2.1 The College operates a number of social media accounts on various platforms. Social media is an important part of how the College communicates and interacts with its employees, students and other stakeholders. Students with responsibility for contributing to the College's social

media activities, for example the Student Union executive, must be mindful at all times that they are representing the College.

- Official postings to official college sites are to be made only when specifically authorised to do so by the Principal or member of SLT.
- Students may contribute to or interact with any posting on an official account subject to the terms of this policy (e.g., 're-tweeting' a message or 'liking' or adding a comment to a posting.
- Where any negative posting about the College, its employees or work is made on a social networking site (whether a college account or otherwise), students should not reply or react to the posting in any capacity. They should bring it to the attention of the Head of School, Learning Technologist or Head of Student Experience.
- If a student group wishes to create a social media account to use for college business, they must get the approval of a member of the Senior Leadership Team and the Head of Marketing and Communication.
- The Head of Marketing and Communication will keep a register of college accounts and monitor their use, ensuring that it is appropriate to the College's communication strategies, reputation and standing.
- Students must not create an account on any social media platform under a name similar to that of the College, or that could in any way be associated with or confused with an official College account.

5.0 Expected Standards of Conduct on Social Media Websites

5.1 Appropriate conduct

5.1.1 In preparation for employment students will be provided with guidance of appropriate conduct in relation to the use of social media, through the curriculum and tutorials. This will include the importance of:

- Conduct themselves in accordance with policies, procedures and Code of Conducts.
- Being professional, courteous and respectful as would be expected in any other situation.
- Think carefully about the impact of any posting or contribution made on social media sites.
- Gaining consent when posting information or images that involves others
- Removing any inappropriate postings, comments, images or videos about themselves or others.

5.2 Inappropriate conduct

5.2.1 When communicating through social media students **must not** conduct themselves inappropriately. The following are examples of inappropriate conduct:

- Engaging in activities that have the potential to bring the College into disrepute.
- Breach of confidentiality by disclosing privileged, sensitive and/or confidential information.
- Making comments that could be considered to be bullying, harassing or discriminatory.
- Doing anything that may conflict with the interests of the College.
- Posting remarks which may reasonably be considered to cause offence.
- Posting or uploading inappropriate comments, images, photographs or video clips about staff, students or ex-students, parents, clients or any other stakeholder of the College.
- Publishing defamatory opinions or information and/or false material about the College, staff or other students.

- Creating an account or posting material purporting to come from a member of staff, student or any other individual. This includes creating an account that could reasonably be confused with the College.
- Posting a comment or opinion that purports to represent the views of the College, unless approved by the member of staff responsible for the College's social media accounts.
- Posting material which may contravene the College's equality and diversity policy.
- Use of offensive, derogatory or intimidating language which may damage student relationships.
- Behaviour that would not be acceptable in any other situation.
- Knowingly accessing or downloading material which is illegal.
- Posting any material that breaches copyright legislation.
- Using a college email account to create a personal social media account.
- Using social media websites in any way which is deemed to be unlawful.

5.2.2 The above examples are not exhaustive or exclusive.

5.2.3 Students will be held personally liable for any material published on social media websites that compromise themselves, their colleagues and/or the College.

6.0 Relationships on Social Media Websites

6.1 The College encourages the positive use of social media as part of the educational process. Social media are used by many people, particularly students to communicate with their peers and the **public** and by the College itself, on official, rather than personal pages of websites such as Facebook. However, students should be aware that employees must not form personal relationships with any students, or ex-students under the age of 18, or parents of current students and must ensure that professional boundaries are maintained at all times.

6.2 Any safeguarding concerns of acts of a criminal nature will be referred to the College's Designated Safeguarding person and may subsequently be referred to the police, Local Safeguarding Children Partnership (LSCP) and/or the Independent Safeguarding Authority (ISA).

7.0 Responsibilities

7.1 All students are responsible for complying with the requirements of these guidelines.

7.2 If Students have concerns about information or conduct on social media sites that are inappropriate, offensive, demeaning or could be perceived as bullying, this should be reported to their tutor immediately.

8.0 Cyber Security

Richmond upon Thames College is certified to meet the following Cyber Security standards:

- Cyber essentials certificate number IASME-CE-024084
- Cyber essentials Plus certificate number IASME-CEP-006200