

eSafety Policy

Reference Number: LEA34

Version: 8

Page(s):	8
Approved SMT Date:	25/09/2025
Last Review Date:	14/07/2026
Review Frequency:	Annually
Next Review Date:	31/07/2027
Originator title:	Vice Principal – Quality Improvement
Author:	Deputy Principal Quality and Student Services
Equality Impact Assessment Date:	29/09/2025
Equality Impact Assessment Review Date:	30/09/2028
Associated Policies:	AI Policy CRC Professional Boundaries Data Protection Policy Harmful Sexual Behaviours Policy IT Systems Acceptable Use Policy Safeguarding and Child Protection Policy Student Regulations

1. Background

This policy document outlines the College's approach to eSafety in accordance with best practice in the FE Education sector. This policy has been written to provide guidance to staff regarding any online or technological communications with students or colleagues.

The College is required under the DfE's statutory guidance, '**Keeping Children Safe in Education**' to keep students safe online whilst at College. This includes ensuring students are aware of the risks of accessing digital information and using digital platforms, and providing regular training and guidance to staff. It also includes the use of appropriate filters and monitoring systems to limit exposure to potential risks and inappropriate or harmful content while using the College's IT systems.

2. Scope

The policy applies to all members of the College's community who have access to the College's IT systems, both on the premises and remotely. The eSafety Policy applies to all uses of the internet and electronic communication devices such as e-mail, mobile phones, video conferencing, social media platforms and messaging services, apps, online games, and any other systems that use the internet for communication and information storage

3. Aim

CRC recognises that social media and other forms of technology not only provide great opportunities but also create risks. The College uses a blend of online and face-to-face delivery and communication tools, and it is crucial that staff use this technology responsibly and that there is a policy in place to support and encourage responsible use.

CRC takes seriously its statutory duty and responsibility to safeguard and promote the safety and welfare of children, young people and those adults deemed 'vulnerable' and/or 'susceptible'. Our approach is to implement safeguards and to support staff and students to identify and manage risks independently. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies. In furtherance of our duty to safeguard students, we will do all that we can to make our students and staff stay e-safe and to satisfy our wider duty of care. This policy forms part of the 'Preventative Education' strand of our Safeguarding and Child Protection Policy

The key mechanisms for ensuring that information about eSafety is delivered, checked and reinforced include:

- Student, adult learner and apprentice induction
- Group tutorials
- T Mail, ACE projects and other personal development materials
- Guidance and materials provided for student self-access, for example via Virtual Learning Environments.
- Apprenticeship progress review meetings
- Teaching and learning sessions at college, in the workplace and online

This eSafety Policy outlines how best to use technology to the professional benefit of the College, its staff and students. The College would like to ensure that members of staff follow the same professional standards online as they would in real life

This eSafety policy should be read in conjunction with CRC Professional Boundaries, the Safeguarding and Child Protection Policy, the Safeguarding Handbook, the IT Acceptable Use Policy, Student Regulations, the AI policy and the Data Protection Policy. Any member of staff found to be in breach of this policy may be subject to disciplinary processes.

4. Roles and Responsibilities

Students and apprentices will:

- be provided with information on how to use the internet and other digital technologies safely and responsibly during induction
- be shown how to use the internet and other digital technologies to support, extend and enhance their learning, including by accessing online learning sessions and materials on the VLE and other platforms
- develop an understanding of intellectual property and copyright
- develop skills to effectively use the internet for research purposes
- develop skills to evaluate information on the internet, including an awareness of online risks, including misinformation, disinformation and conspiracy theories
- understand how to use AI tools safely and ethically, to support their learning without compromising their assessment by inappropriate use
- be shown how to report eSafety concerns to their tutor or assessor/trainer or to a member of the Student Services Team.

Tutors and assessor/trainers will:

- deliver an effective induction in line with central college induction plans, using the materials provided by the eLearning and Student Services teams
- ensure that students have the information they need to access online learning safely
- ensure that students know what to do if they have a concern about eSafety, or concerns about online material

Lecturers and assessor/trainers will:

- work with students and colleagues to ensure that students develop an understanding of how to access, evaluate, research and use online tools safely

Leaders and managers will:

- ensure that information about eSafety is available to all staff and students
- ensure that support and guidance on safe use of IT is provided to all staff and students
- ensure that college IT equipment is maintained to a safe standard
- ensure that measures are in place to ensure data is safe and secure and access to unsuitable content is disabled in line with the IT Acceptable Use and Cyber Security policies

All staff:

- are responsible for ensuring the safety of students
- should report any concerns immediately to their line manager or to a member of the Safeguarding team in line with the Safeguarding and Child Protection policy
- When informed about an eSafety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

- Should model safe, responsible and professional behaviours in their own use of technology in college and in their personal use.

5. Student Conduct

As members of the College community, students must abide by the rules and values of the college, respecting the rights of fellow students and staff, as well as the reputation of the college. Students must not post comments on social media or online, or send text or other online messages that are in breach of Student Regulations including those:

- That are unlawful
- That could be viewed as bullying or harassing another member of the college community
- That are contrary to the College's Equality and Diversity policy
- That explicitly encourage other members of the College community to break the law
- That are likely to bring the college into disrepute

Students should not post photos of a sexual nature. If a staff member becomes aware of a situation where this has arisen, they should follow the procedure outlined in the Safeguarding and Child Protection Policy and log a concern via the Safeguarding team.

Students should not contact or make communication to a staff member via a social network. This includes attempting to add a member of staff as a 'friend'.

Students will be given guidance on appropriate use of the internet, AI and eSafety through induction, group tutorial and the VLE.

If a student has cause for concern regarding use of the internet or social media, they should report the incident immediately to a member of staff. There may be occasions where this will be treated as a safeguarding issue.

6. Staff Conduct

6.1 Use of Social Media

Safeguarding students is a key priority for the College and, as such, the use of social media as a means by which members of staff communicate with students requires clear guidance on appropriate use. The College has in place a Social Media Policy which details the expectations of staff.

6.2 Communication with Students and Colleagues

Communication between students and colleagues, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phone text messaging, emails, social media, video conferencing such as Teams or Zoom and messaging services.

Social Media groups or microsites set up on behalf of the College, for example a departmental Facebook or other social media group must be with the prior consent of the Director of Marketing who will keep a record of these groups and provide guidance on safe and professional use. Groups will be subject to monitoring by the Marketing department. All such groups and microsites must comply with college Safeguarding and Child Protection, Data Protection and IT Acceptable Use of IT Policies. Use of images must be in strict compliance with the policy on Consent to Share Personal Information with a Third Party,

6.3 Staff with Students as social media “friends”

The College position is that staff should not befriend students on social media because professional boundaries may be misconstrued. However, the College recognises that some members of staff may have family members, partners and/or friends, who are students at the College. These staff may therefore have a student as a “friend” on their social network site and as such should inform their line manager so a record can be made. In these circumstances staff should also take responsibility for ensuring that pictures and comments on social networks are not professionally damaging. Young Apprentices working at the college, with friends who are students at the College, should be aware of their conduct online now that they have the same professional responsibilities as other members of staff.

6.4 Cyberbullying

Cyberbullying is the use of Information and Communications Technology (ICT), particularly mobile phones, Teams, social media and the internet, to deliberately upset someone. It is recognised that staff in college, as well as students, may become targets of cyberbullying. Like other forms of bullying, cyberbullying can seriously impact on the health, well-being, and self-confidence of those targeted. The College does not tolerate any kind of bullying, including cyberbullying, and incidents should be reported and will be taken seriously and addressed immediately. Please refer to the College’s Bullying and Harassment Procedure for Staff and the Student Regulations and Harmful Sexual Behaviours Policy.

6.5 Photographic Images

It is recognised that there are times when photographic images of students may enhance the learning experience or be necessary evidence for coursework. Staff must adhere to the College Data Protection Policy and Third-Party Consent Policies to ensure that images and other personal data is used in accordance with UK GDPR and the Data Protection Act 2018.

7. Data protection

The College is committed to complying with UK General Data Protection Regulations (UK GDPR) and the Data Protection Act 2018. Staff will be provided with training and regular updates in line with our Data Protection Policy.

8. Security

The safe use of technology is a key element to keep students safe including appropriate filters and monitoring of systems in place to protect students from harmful online materials.

All students and staff at Cambridge Regional College have their own personal, password protected, account for use for all College related activities and storage of personal data relating to those activities. All systems in the College have security protection software on them to help prevent loss or corruption of data due to ransomware and virus attacks. All user network data is backed up to ensure we can restore information as and when requested by students and staff.

All students and staff have access to all the latest software to allow them to work easily and comfortably meeting workstation requirements that individuals may have.

The College monitors search terms used on all devices linked to the College’s WiFi system. The College also uses cloud-based software, Senso, which is installed onto College-owned devices for the purpose of filtering and monitoring. Senso uses artificial intelligence to check search terms and the content of every website a student attempts to visit, Senso contains a detections

library of trigger words. Should any of the trigger words be detected the College's safeguarding team are notified for follow up.

The College monitors PCs and laptops in classrooms and workshops for the purpose of teaching, class management and safeguarding. This includes PCs and laptops used for exams and controlled assessments, to ensure exam regulations have been followed.

The College also uses a system to block potentially inappropriate or harmful websites from access from college devices. Computer usage during lessons must be course related at all times.

The College employs a perimeter firewall for the protection of the College's network services, devices. All activity data is kept securely and only accessed on request by authorised members of the IT Services department, safeguarding and data protection teams.

9. Equality and Diversity

As with all College Policies and Procedures due care has been taken to ensure that this policy is appropriate to all employees regardless of gender, race, ethnicity, disability, sexual orientation, marital status, gender identity, religion or age.

The policy will be applied fairly and consistently whilst upholding the College's commitment to providing equality to all.

If any employee feels that this or any other policy does not meet this aim, please contact the College's Director of Human Resources

10. Monitoring arrangements

This policy will be reviewed annually by relevant managers including the Director of Student Services, Vice Principal – People and Commerce, and the college's Designated Safeguarding Lead.

Feedback from students and apprentices will be sought using established Student Voice processes, such as surveys and department boards

Document history

Date	Issue number	Change/Comments	Date Approved	Approved by
30/11/2017	2	Added Student Conduct Security Data Protection Authorised College sites		
28/10/2020	3	Significant updates following move to blended learning	28/10/2020	VPQI
22/07/2022	4	Annual review, no significant changes	22/07/2022	VPQI
28/07/2023	5	Annual review added reference to Prevent and AI policies in associated documents		DPQSS
31/07/2024	6	Annual review – minor changes to job titles and format	01/08/2024	DPQSS
31/07/2025	7	Annual review – minor changes to include references to AI use	25/09/2025	DPQSS
14/07/2026	8	Annual review – minor changes to include reference to ACE Project		

