ALTERNATIVE PROVISION

e-Safety Policy

Approval Date: January 2026

Revision Due Date: January 2027

Approved by: RAISE-AP Educational Directors

Approval Signatures

RAISE-AP
Directors

Table of Contents

Policy Statement

This e-Safety Policy applies to all members RAISE-AP, including students, staff, visitors and contractors who have access to, and are users of ICT systems and resources both in and out of learning venues, e.g. internet, electronic communications, Virtual Learning Environment (VLE) or mobile devices.

e-Safety informs the wider safeguarding agenda, and this policy operates in conjunctions with other polices including Acceptable Use, Behaviour and Data Protection. Where student access ICT through a third party (i.e. students on work placement or enrolled as an apprentice) the polices of the organisation should be followed.

Context

To prepare students for the needs of today and their future working lives where the curriculum and their personal goals require them to learn how to locate, retrieve and exchange information using a variety of technologies. Computer skills are vital to access employment and life-long learning as ICT is now seen as an essential skill for life. However, technologies present risks to vulnerable groups as well as benefits. Internet use for work, home, social and leisure activities is expanding across all sectors of society.

This brings our staff and students into contact with a wide variety of influences some of which may be unsuitable. These new technologies are enhancing communication and the sharing of information, which inevitably challenge the definitions and boundaries of the RAISE-AP environment. Current and emerging technologies in RAISE-AP and more importantly, in many cases used outside the college by students include:

- Internet websites
- Virtual Learning Environments (VLE)
- Instant messaging
- Social networking sites
- e-mails
- Blogs
- Podcasting
- Video broadcasting sites
- Chat rooms
- Gaming and gambling sites
- Music download sites
- Mobile phones with camera and video functionality
- Digital cameras

- Smart phones, iPads and Tablets with e-mail and web applications.
- Microsoft Teams

All of these have potential to help raise standards of teaching and learning but may equally present challenges to both students and tutors in terms of keeping themselves safe.

These challenges include:

- Exposure to inappropriate material
- Cyber-bullying via websites, social media, mobile phones or other technologies
- Identity theft or invasion of privacy
- Downloading copyrighted materials
- Exposure to inappropriate advertising online gambling and financial scams
- Safeguarding issues such as grooming (Children or vulnerable adults)
- Other illegal activities.

Roles and Responsibility

All teaching and non-teaching staff (including volunteers, suppliers, contractors and temporary staff) are responsible for supporting safe behaviour throughout RAISE-AP and following safety procedures.

Staff

All RAISE-AP staff should:

- Participate in any mandatory e-safety training and awareness raising sessions read, understand, accept and act in accordance with the RAISE-AP e-Safety Policy report any suspicion of misuse to the designated persons or line manager.
- Refrain from making negative comments about students or RAISE-AP on any blogs or social networking sites. Negative comments such as these could be considered as gross misconduct as it potentially affects the reputation of RAISE-AP and/or lowers morale.
- Help educate students in keeping safe, acting as a good role model in their own use of ICT and directing to sites which are appropriate for the use of learning.
- Be vigilant in monitoring the content of websites in case there is any unsuitable material
- Be aware of the potential for cyber-bullying in their sessions where malicious messages e.g. through the use of forums on the VLE and social networking sites, or via internal class emails or text messages on mobile phones etc, which can cause hurt or distress.

Students

Students are encouraged to access various technologies in sessions, private study and in the completion of assignments and independent research and are therefore expected to follow the RAISE-AP Acceptable Use Policy. They should participate fully in e-Safety activities and report any suspected misuse to a member of staff. Students are required to sign an agreement to state that they agree to the terms of our Acceptable Use Policy and their e-safety responsibilities.

Code of Conduct

Students & Staff are expected to:

- Behave in a safe and responsible manner.
- Treat equipment with respect.
- Store college data only on college authorised Cloud storage Microsoft One Drive for business.
- Be polite and not use e-mail, social media or blogs etc to make negative comments, bully or insult others.
- Use the resources only for educational purposes.

Students & Staff are expected not to:

- Waste resources including Internet and printers
- Eat or drink when using ICT resources
- Use someone else's login details or share your own
- Have any inappropriate files (e.g. copyrighted or indecent material)
- Attempt to circumvent or "hack" any systems
- Use inappropriate or unacceptable language
- Reveal their personal details or passwords
- Visit websites that are offensive in any way
- Use chat rooms or newsgroups, apart from the VLE site
- Do anything that could damage the reputation of RAISE-AP
- Download anything inappropriate or install any unauthorised software's.
- Store college data on any other cloud storage.

Breaching these Rules may lead to:

- Withdrawal from the RAISE-AP ICT facilities.
- Temporary or permanent prevention of access to the relevant pages on the Internet.

- Limited or disabled rights where systems are relevant.
- Appropriate disciplinary action under the college behaviour policy.
- Users should note that breaches of the provisions set out in these Rules may lead to criminal or civil prosecution.

System Security

Prior to commencing employment at RAISE-AP all users must read and agree to the RAISE-AP 'ICT Acceptable usage Policy'.

All IT equipment / computer systems are owned by RAISE-AP and have appropriate software/filtering to ensure safe internet use. RAISE-AP Educational Directors will be responsible for systems support and will ensure that the appropriate filters are applied to the equipment in the college.

If staff or students discover unsuitable sites have been accessed on the college IT equipment, they must report their findings to RAISE-AP Educational Directors so that filters can be reviewed. RAISE-AP reserves the right to examine or delete any files that may be held on its system or to monitor any internet sites visited.

Alerting

Once you suspect or know of any e-Safety issues, you should contact a Safeguarding Officer immediately. In the event of immediate danger staff should contact the police (999) and inform the RAISE-AP Educational Directors.

Monitoring and Reviewing

This Policy will be reviewed annually in line with the RAISE-AP quality systems.

Raise Values

Our RAISE-AP values (Resolve, Attitude, Invest, Social Skills and Education) are key in everything we do, specifically with attitudes (modelling and expectations), invest (tailoring setup for our young people) social skills (becoming part of a community) which are linked to our e-Safety policy.
