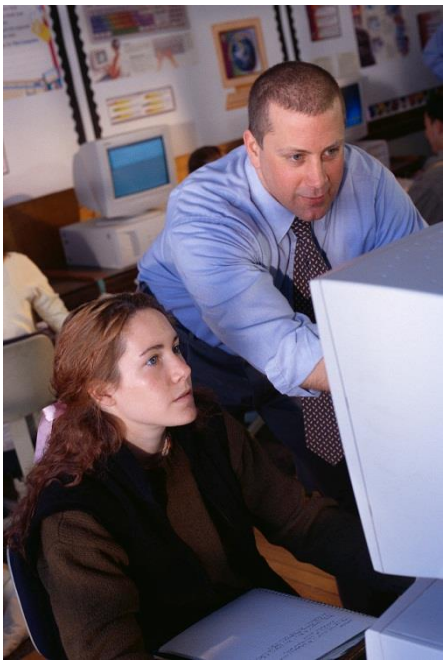
Action Community Enterprises CIC (ACE)

E-Safety Policy



Policy number:	
Version:	1.0
Policy holder:	Lou Gardiner
Approval board:	ACE Board of Directors
Date of original approval:	September 2022
Date of latest approval:	September 2024
Review period:	Annually
Date of next review:	September 2025

Background / Purpose

This policy is part of the comprehensive approach adopted by Action Community Enterprises (ACE) towards safeguarding students and should be read in conjunction with the of safeguarding policy.

This policy allows ACE to demonstrate that it not only acknowledges eSafety as an important issue for our learning communities, but also that we have made a considered attempt to embed eSafety into our approach to learning using technology.

The Policy applies to all members of the ACE community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of ACE digital systems, both in and out of the centres. It also applies to the use of personal digital technology on the ACE sites (where allowed).

Keeping Children Safe in Education 2023 clearly states that:
It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **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.
- **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. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

Policy Objectives

To ensure everyone in the ACE learning community has the opportunity to develop a set of safe and responsible behaviours that will enable them to reduce the risks, whilst continuing to benefit from, the opportunities of using technologies.

Procedure and Practices

ACE believes that eSafety is the responsibility of the whole learning community and everyone has a part to play in ensuring technology is used safely.

The following responsibilities demonstrate how each member of the ACE community will contribute to eSafety:

The CEO and Managing Director will:

- Develop and promote an eSafety culture within the centres.
- Make appropriate resources, training and support available to centre staff to ensure they are able to carry out their roles with regard to eSafety effectively.
- Review any eSafety incidents and be aware of the procedure to be followed should an eSafety incident occur.
- Develop an understanding of current eSafety issues, guidance and appropriate legislation.
- Ensure that eSafety education is embedded across the curriculum.
- Take ultimate responsibility for the eSafety of their Centre/provision.
- Monitor and report on eSafety issues to the Local Advisory Board.
- Take responsibility for the security of the centres ICT system.
- Ensure that eSafety is promoted to parents and carers.

Students will be encouraged to:

- Read, understand and adhere to the ACE policy and practices in relation to eSafety.
- Help and support the centre in creating eSafety policies and practices.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies in the centre and at home.
- Take responsibility for their own and each other's safe and responsible use of technology in the centre and at home, including judging the risks posed by the personal technology owned and used by students outside of the centre.
- Respect the feelings, rights, values and intellectual property of others in their use of technology in the centre and at home.
- Understand what action should be taken if they feel worried, uncomfortable, vulnerable or at risk whilst using technology in the centre and or at home, and if they know of someone who this is happening to.
- Discuss eSafety issues with staff, family and friends in an open and honest way.

ACE Staff will:

- Read, understand and help promote the ACE eSafety policy.
- Develop and maintain an awareness of current eSafety issues and guidance.
- Model safe and responsible behaviours in their own use of technology.
- Embed eSafety messages in learning activities where appropriate.
- Supervise students carefully when engaged in learning activities involving technology.
- Be aware of what to do if an eSafety incident occurs.
- Communicate in a professional capacity and ensure that the technologies used are officially sanctioned by ACE
- Ensure that any digital communication between staff and students or parents/carers (e-mail, social media, learning platform, etc.) are professional in tone and content.
- Follow good practice when using personal social media regarding their own professional reputation and that of ACE and its community
- Immediately report to a CEO the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication

Parents and Carers will be encouraged to:

- Help and support the centre in promoting eSafety.
- Read, understand and promote the ACE eSafety policy.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in the centre/provision and at home.
- Discuss eSafety concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in their own use of technology.
- Contact the centre if they have any concerns about their child's use of technology.

Local Advisory Board will:

- Contribute to and help promote ACE's eSafety policies and practices.
- Develop an overview of the benefits and risks of the internet and common technologies used by students.
- Develop an overview of how the ACE ICT infrastructures provides safe access to the internet.
- Develop an overview of how the centres encourage students to adopt safe and responsible behaviours in their use of technology in and out of the centre.
- Review the impact of the eSafety policy.

Learning and Teaching

- At ACE, we believe that the key to developing safe and responsible behaviours online, not only for students but for everyone within our learning community,

lies in effective education. We know that the internet and other technologies are embedded in our students' lives not just in the centre but outside as well, and we believe we have a duty to help prepare our students to safely benefit from the opportunities the internet brings.

- We will discuss, remind or raise relevant eSafety messages with students routinely wherever suitable opportunities arise during lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

Managing ICT Systems and Access

- The centres will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up-to date.
- The centres will agree which users should and should not have internet access, and the appropriate level of access and supervision they should receive.
- Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the centre ICT systems, and that such activity will be monitored and checked.
- Students will access the internet using an individual log-on, which they will keep secure. Whether supervised by a member of staff, or working independently, students will abide by the Appropriate Use Protocols (APU) at all times.
- Members of staff will access the internet using individual log-on, which they will keep secure. They will ensure they log out after each session, and not allow students to access the internet through their log-on. They will abide by the AUP at all times.
- Any administrator or master passwords for centre ICT systems will be kept secure.
- The centres will take all reasonable precautions to ensure that users do not access inappropriate material. However, it is not possible to guarantee that access to unsuitable material will never occur.
- ACE will regularly audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate. We will regularly review our internet access provision, and review new methods to identify, assess and minimise risks.
- ACE use a recognised/validated filtered internet service.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the Managing Director.

- If users discover a website with potentially illegal content, this should be reported immediately to the Managing Director Manager.
- The centre will regularly review the filtering and other security systems to ensure they meet the needs of all users.

Using Email

- Staff and students should use approved email accounts allocated to them by the centres and be aware that their use of the ACE email system will be monitored and checked.
- Students will be allocated an individual email account for their use in the centres.
- Students will be reminded when using email about: the need to send polite and responsible messages; the dangers of revealing personal information, the dangers of opening email from an unknown sender; or viewing/opening attachments.
- Communication between staff and students or members of the wider learning community should be professional and related to centre matters only.
- Any inappropriate use of the ACE email system, or the receipt of any inappropriate messages by a user, should be reported to the CEO/Managing Director

Using images, video and sound

- Staff will remind students of safe and responsible behaviours when creating, using and storing digital images, video and sound. They will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at the centre/provision and at home.
- Staff and students will follow ACE practices on creating, using and storing digital resources. In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online without permission of the staff/students involved.
- If students are involved, relevant parental permission will also be sought before resources are published online.

Using blogs, wikis, podcasts, social networking and other ways for students to publish content online

- Blogging, podcasting and other publishing of online content by students will take place within the ACE learning platform blog. Students will not be allowed to post or create content on sites where members of the public have access.
- Any public blogs run by staff on behalf of ACE will be hosted on the learning platform/ACE website blog and postings should be approved by the Managing Director before publishing.

- Students will model safe and responsible behaviour in their creation and publishing of online content within the ACE learning platform. For example, students will be reminded not to reveal personal information which may allow someone to identify and locate them. Students will not use their real name when creating such resources. They will be encouraged to create an appropriate 'nickname'.
- Staff and students will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking and other online publishing outside of the centre/provision.

Using video conferencing and other online video meetings

- All video conferencing activity will be supervised by a suitable member of staff.
- Students will not operate video conferencing equipment, or answer calls, without permission from the supervising member of staff.
- Video conferencing equipment will be switched off and secured when not in use/online meeting rooms will be closed and logged off when not in use.
- Students will be given appropriate user rights when taking part in an online meeting room. They will not have host rights of the ability to create meetings rooms.
- Video conferencing should not take place off centre premises without the permission of the Managing Director.
- Permission will be sought from all participants before a video conference is recorded. Video conferences should only be recorded where there is a valid educational purpose for reviewing the recording. Such recordings will not be made available outside of ACE.

Using mobile phones

- Where staff members are required to use a mobile phone for ACE duties, for instance in the case of an emergency during off-site activities, or for contacting students or parents, then a ACE mobile phone should be provided and used. Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a student or parent.

Protecting personal data

- The CEO will ensure personal data is recorded, processed, transferred and made available according to the Data Protection act (2018) and GDPR (2018).
- Staff will ensure they properly log off from a computer terminal after accessing personal data.
- Staff will not remove personal or sensitive data from ACE premises without permission of the Managing Director and without ensuring such data is kept secure.

Dealing with eSafety incidents

The CEO will respond appropriately to safety incidents. Depending on the nature of the incident, the CEO will discuss what action to take with: the designated member of the Local Advisory Body seeking advice from external agencies.

ACE takes all reasonable precautions to ensure online safety for all centre users but recognises that incidents may occur inside and outside of the centre (with impact on the centre) which will need intervention. ACE will ensure:

- there are clear reporting routes which are understood and followed by all members of the ACE community which are consistent with the ACE safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the ACE community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm the incident will be escalated through the agreed ACE safeguarding procedures.