E-Safety Policy

Version Control						
Version	Author	Date	Changes	Approval	Approval Date	Review Date
1.1	E Merrick	06/09/22	Policy creation	DW	07/09/22	06/09/2022
1.2	D Priestley	04/09/23	Policy review	DW	04/09/23	04/09/2024
1.3	D Priestley	04/09/24	Policy review	DW	04/09/24	04/09/2025
1.4	D Priestley	02/09/25	Policy review	DW	03/09/25	02/09/2026

A2L E-Safety Policy

Introduction

At Aim2Learn Ltd (A2L) we believe that ICT is central to all aspects of learning. A2L will always strive to ensure our provision should reflect the rapid developments in technology.

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of young people and adults. Consequently, A2L need to build in the use of these technologies in order to equip our learners with the skills to access lifelong learning and employment.

All Learners, whatever their needs, will have access to a range of up to date technologies in both the ICT suite and classrooms. ICT is a key life skill and should not be taught in isolation.

Information and Communications Technology covers a wide range of resources, including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies being used both inside and outside the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

All users need to be aware of the range of risks associated with the use of these Internet technologies.

At A2L we understand the responsibility we have to embed awareness on e-safety issues, teaching learners the appropriate behaviours and critical thinking skills to enable them to remain both safe and legally compliant when using the internet and related technologies, in and beyond the context of the training room.

This e-safety policy reflects the need to raise awareness of the safety issues associated with information systems and electronic communication as a whole.

All staff are familiar with the A2L policy, including:

- safe use of e-mail
- safe use of the Internet
- safe use of our Network/LAN, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of Learners information/photographs for marketing purposes
- procedures in the event of misuse of technology by any member of A2L, Staff or trainee (see appendices)
- their role in providing e-safety education for learners.

Staff are updated about e-safety regularly and new staff and learners receive information on A2L's acceptable use policy as part of their induction.

E-safety within the training environment

ICT and online resources are increasingly used across the curriculum. A2L believe it is essential for e-safety guidance to be given to learners on a regular and meaningful basis. We continually look for new opportunities to promote e-safety.

- A2L provide opportunities, embedded within the programme to teach about e-safety.
- Educating Learners on the dangers of technologies that may be encountered in a training environment, which is also transferable into employment and personal life.
- Learners are taught about copyright and respecting other people's information, images, etc. through discussion, modelling, and activities are embedded throughout programme.
- Learners are made aware of the impact of online bullying and 'Trolling' and are encouraged on where to seek help if they are affected by these issues. Learners are also aware of where to seek advice or help if they experience problems when using the internet and related technologies (cyber bullying)
- Learners are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Telecoms and ICT curriculum
- Learners are taught about the risks inherent in using social media, with particular emphasis of sharing data, personal images and information (GDPR)

Managing Internet Access

Learners will be given access to Internet resources whilst in centre.

- Raw image searches are discouraged when working with learners.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the tutor.
- Our internet access is controlled through firewalls and web filtering service.
- If staff discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the Centre Manager
- It is the responsibility of A2L, by delegation to the centre manager, to ensure that antivirus protection is installed and kept up-to-date on all Learning machines.

E-mail

The use of email within our centre is essential means of communication for staff, and is a requirement for evidence withing the BTEC Portfolio. In the context of Learning, email should not be considered private.

Educationally, email can offer significant benefits including, direct written contact between Learner and Tutor on different projects. A2L recognise that Learners need to understand how to style an email in relation to formal and informal communications.

- Learners are introduced to email as part of evidence gathering for their BTEC portfolios.
- A2L give staff their own email account, to use for all business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Under no circumstances should staff contact Learners using personal email addresses.
- The forwarding of chain letters is not permitted.
- All learners must use appropriate language in e-mails and must not reveal personal details of themselves or others in e-mail communication.

Publishing Learners images and work

All learners will be asked to give permission for their photos to be taken and to use their work/photos/video in the following ways:

- on A2L web site
- in display material that may be used in communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the Provider
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically.)

Learners' names will only be published alongside their image and vice versa with expressed permission.

Social networking and personal publishing

Social Networking will be encouraged for the purposes of Job searching and professional networking on sites such as LinkedIn, Learners will be advised that the use of social network spaces outside of training will not be monitored by A2L in any way – and any view or opinion expressed, belong to those of the individual and not A2L.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

- Mobile phones will not be used during formal Lesson times. The sending of abusive or inappropriate text messages is forbidden.
- All Learners will be permitted to use their own personal Laptops within classrooms for the purpose of making assessment notes, write ups of evidence. emails, educational applications.

Data protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and UK GDPR 2018.

Data Protection Act 2018

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals rights of access to their personal data, compensation and prevention of processing. Data protection: The Data Protection Act - GOV.UK (www.gov.uk)

Responding to e-safety incidents/complaints

A2L will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a Training computer or mobile device. We cannot accept liability for material accessed, or any consequences of Internet access. Complaints relating to e-safety should be made to a member of the training team. Any complaint about staff misuse must be referred to the Centre Manager.

- All users are aware of the procedures for reporting accidental access to inappropriate materials. Any breach must be immediately reported.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged and, depending on the seriousness of the offence; investigation by the Centre Manager, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences
- Learners will be informed of the complaints procedure.
- Learners will need to work in partnership with staff to resolve issues.

Cyberbullying

Cyberbullying is the use of ICT, particularly mobile phones and the internet, to deliberately upset someone else. A2L has a duty to protect all its members, staff and learners, providing a safe, healthy environment. Although bullying is not a specific criminal offence under UK law, there are laws that can apply in terms of harassing or threatening behaviour, for example, or indeed menacing and threatening communications.

Preventing Cyberbullying

It is important that we work in partnership with learners, and parents/careers where applicable, to educate them about Cyberbullying as part of our e-safety curriculum. They should:

- understand how to use these technologies safely and know about the risks and consequences of misusing them
- know what to do if they or someone they know are being cyber bullied.
- report any problems with Cyberbullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

Additional online advice on how to react to Cyberbullying can be found on www.wiredsafety.org

Supporting the person being bullied

Support can be given in a variety of ways, including:

- Giving reassurance to the person that they have done the right thing by telling someone
- Help the person keep relevant evidence for any investigation (taking screen capture shots, not deleting messages, diary of incidents)
- Check the person knows how to prevent it from happening again e.g. blocking contacts, changing contact details.
- Take action to contain the incident when content has been circulated: remove content, contact the host (social networking site) to get the content taken down, use disciplinary powers to confiscate phones that are being used to cyber bully – ask the learner who they have sent messages to.

Investigating Incidents

All bullying incidents should be recorded in the incident log and investigated in the same manner as any other bullying incident, in line with the Anti-Bullying and Harassment policy.