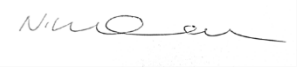
E-SAFETY POLICY

POLICY APPROVAL

Approval Required	Indicate with a tick (✓)		**Annual Review Required**	Indicate with a tick (✓)	
	Yes ✓	No		Yes ✓	No
Approval Panel					
Approved by: **Chair of the Board**	Name: Nikki Witham		Signature: 	Date: 17 January 2022	
Policy Review Date	30 May 2023				
Reviewed by: **Chair of the Board**	Name: Nikki Witham		Signature: 	Date: 30 May 2023	
Next Review Date	April 2024				

INTRODUCTION

Aspire Training Solutions recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and success.

However, the accessibility and global nature of the internet and different technologies mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies.

As part of our duty to safeguard our learners, we will do everything possible to make our learners and staff stay safe online and to satisfy our wider duty of care.

SCOPE

The policy applies to all learners and staff who have access to our IT systems, both on the premises and remotely. Any user of our IT systems must adhere to and accept the Acceptable Use Agreement. The e-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phones, social media, instant messaging, webinar and video conferencing etc.

DEFINITION

The term e-safety is defined for the purposes of this document as the process of limiting the risks to children, young people and vulnerable adults when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and inspection. E-safety risks can be summarised under the following three headings:

CONTENT

- Exposure to age-inappropriate material
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance, sites promoting radicalisation or pornography
- Exposure to illegal material, such as images of child abuse
- Illegal downloading of copyrighted materials e.g. music and films

CONTACT

- Grooming using communication technologies, potentially leading to sexual assault, child sexual exploitation and radicalisation
- The use of assumed identities on gaming platforms
- Bullying via websites, mobile phones or other forms of communication device
- Spyware, e.g. use of Remote Access Trojans/Tools to access private information or spy on their victim.

COMMERCE

- Exposure of minors to inappropriate commercial advertising
- Exposure to online gambling services
- Commercial and financial scams

RESPONSIBILITIES

The Senior Leadership Team are responsible for maintaining this policy. The following are responsible for implementing it:

The Safeguarding and Prevent Designated Lead is responsible for:

- Keeping up to date with new technologies and their use, as well as attending relevant training.
- SourcIng and make accessible staff development and training
- Recording incidents
- Reporting any developments and incidents and liaise with the local authority and external agencies to promote e-safety.
- Providing pastoral and practical support for learners dealing with issues related to e-safety.

The Curriculum Lead for:

- Championing good e-safety practice in IT facilities and processes
- Incorporating e-safety into learner induction

Delivery Team for:

- Embedding e-safety education and practice into their teaching programme.

All staff for:

- Staying alert to and responding appropriately to any potential or actual e-safety issue.

SECURITY

Aspire Training Solutions will do all that it can to make sure the network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, workstations to prevent accidental or malicious access of our systems and information.

Digital communications, including email and internet postings, over the network, will be monitored in line with the Acceptable Use Policy. Aspire Training Solutions complies with guidelines set out by the Counter Terrorism Internet Referral Unit (CTIRU) and has a statutory duty to ensure their systems cannot be used to access any of the websites on the CTIRU list.

BEHAVIOUR

Aspire Training Solutions will ensure that all users of technologies adhere to the standard of behaviour as set out in the Acceptable Use Policy. We will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary procedures.

USE OF IMAGES AND VIDEO

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or learners. All learners and staff should receive training on the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted onto social networking sites, for example. Aspire Training Solutions teaching staff will provide information to learners on the appropriate use of images as detailed in the Acceptable Use Policy. This includes photographs of learners and staff as well as using third party images.

Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe. No image/photograph can be copied, downloaded, shared or distributed online without permission from the owner.

E-SAFETY GUIDELINES

- ✓ Keep your personal information private – avoid sharing personal information such as your phone number, home address or photographs with people you don't know in person and trust.
- ✓ Check whether the social media networks you use allow you to create friend lists. These lists let you manage who sees what. For example, you may only want your closest friends to see some information.
- ✓ Use private messages for people you know in person and trust; be careful of private messaging people you don't know.
- ✓ Use a strong and unique password for all of your online accounts – a combination of letters, numbers and symbols (and if you've ever shared it in the past, CHANGE IT).
- ✓ Know how to block someone if they make you feel uncomfortable or upset.
- ✓ Learn how to save chat logs and texts so that if someone does make you uncomfortable or upset, you have evidence to report them.
- ✓ Remember to log out of a site properly after use, especially on a shared computer.
- ✓ Keep your clothes on when using webcam – images of you could end up in the wrong hands!
- ✓ Think very carefully about meeting someone face to face who you only know online –NEVER do this alone, always talk to your parents or carers before you go ahead with this and take a trusted adult friend along with you.
- ✓ Learners or staff should report any abusive behaviour immediately to the Safeguarding and Prevent Officer

GUIDELINES FOR LEARNERS (SOCIAL MEDIA)

As part of our duty of care to our learners, Aspire Training Solutions sets out guidelines below:

- ✓ Do not enter into a "friends" relationship online with someone you do not know.
- ✓ Do not use social media to harass, threaten, insult, defame or bully another person or entity; to violate any policy; or to engage in any unlawful act, including but not limited to gambling, identity theft or other types of fraud.
- ✓ Do not access or participate in social media which insights hatred or promotes radicalisation.
- ✓ Set up privacy settings carefully, ensure you are not sharing any information that you do not want to and check these on a regular basis.
- ✓ Participating in social media use as part of a course activity is optional.

When posting on sites linked to Aspire Training Solutions or when mentioning or to us on social media media do not:

- ✓ Use foul or abusive language
- ✓ Harass, threaten, insult, defame, blackmail or bully another person
- ✓ Refer to any other member of the Aspire Training Solutions community, whether student or staff, in a derogatory or insulting manner
- ✓ Post or comment in any way that reflects poorly on Aspire Training Solutions or is deemed to interfere with the conduct of our Business
- ✓ Posting of messages that are deemed inappropriate will be dealt with under the learner disciplinary procedure
- ✓ Copies of inappropriate posts may be reported to parents/ guardians and the appropriate authorities.
- ✓ Before you post a message, think carefully about its content and ask yourself how you would feel if you received that message or know that it may be disclosed in court
- ✓ Any form of abuse or cyber-bullying will be dealt with under the student disciplinary procedure

GUIDANCE FOR STAFF

This policy sets out guidelines for staff, below, for the use of social media. These guidelines apply to: Posting to any Aspire Training Solutions social media site; communicating with members of the Aspire Training Solutions community including staff or learners; discussing Aspire Training Solutions on any site; whether at one of our centres and using the network and equipment or through a personal account or using a personal phone, computer or other device from any other location.

Staff should follow the guidelines below at all times:

- ✓ Be professional; as a Aspire Training Solutions employee you are an ambassador for the organisation.
- ✓ Never have a "friend" relationship with a learner, where personal details are shared
- ✓ If the Social Media requires a login, create a separate "work" login and ensure any privacy settings are set appropriately so that no personal information can be viewed.
- ✓ Staff should not share any personal information online including home address, personal telephone numbers, personal email addresses or date of birth.
- ✓ When communicating with learners who are under 18 via email, where possible, Aspire Training Solutions learner email addresses should be used.
- ✓ Email communications with learners under 18 must happen within normal working hours (8.30 – 5pm).
- ✓ Do not access or participate in social media which insights hatred or promotes radicalisation.
- ✓ Do not post a person's photograph or video image without first obtaining permission and signed release forms from anyone depicted in the photograph or video (any photographs of children and young people under the age of 16 should have parental permission).