Acceptable use of IT and e-Safety Policy

aspiration TRAINING LTD

ATL Acceptable Use of It and e-Safety policy

Document status:	Final
Date:	October 2021
Review date:	October 2022
Version:	ATL 1.0
Owner:	Director of ICT
Approval Board:	Board of Directors

Contents Page

1. Policy intent:

Aspiration Training recognises the importance of ICT and the internet as highly effective tools for teaching, learning and assessment as well as for carrying out work tasks effectively and efficiently. However, it is important that the use of ICT and the internet is seen as a responsibility and that learners, staff and other key stakeholders use it appropriately and practice good e-safety. It is important that all members of Aspiration Training staff, learners, employers and other key stakeholders are aware of the dangers of using the internet and how they should conduct themselves online. This policy is intended to ensure that all users of Aspiration Training IT services and equipment are able to protect themselves whilst using this equipment, as well as ensuring compliance with other legal and statutory obligations to ensure the integrity and security of Aspiration Training data, systems, contract security standards and ICT equipment.

This policy also provides comprehensive guidance on the acceptable use of Aspiration Training ICT equipment, systems and networks in order to keep these and all Aspiration Training IT users safe and secure and applies to all physical and electronic information assets for which Aspiration Training is responsible.

The key aims of this policy are to:

- To provide all Aspiration ICT users information and guidance to proactively safeguard themselves and others from harm, including the potential for radicalisation
- To ensure compliance with, in conjunction with other policies and procedures, the Prevent Duty as required by the Counter-Terrorism and Security Act (2015)
- Set out the acceptable use of IT systems and resources by learners and employees.
- Ensure the protection of all Aspiration Training information systems, contract assets and customer data and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems and assets.
- Govern all users use of its equipment, systems and internet within or outside of its network, and covers a wide range of issues surrounding user rights, responsibilities and privileges as well as sanctions connected with computer use.
- Provide a safe and secure information systems working environment for staff, learners and any other authorised users.
- To ensure all Aspiration Training authorised users understand and comply with this policy and any other associated policies.
- Ensure all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.
- To protect Aspiration Training partners and the contract from liability or damage through the misuse of its IT facilities.
- Respond to feedback and update as appropriate, initiating a cycle of continuous improvement.

2. Scope of policy:

This policy is applicable to all staff, learners and third parties who use Aspiration Training ICT equipment, software and systems, including e-portfolios and virtual learning environments (VLEs). It will be communicated to all staff, learners and third parties who use Aspiration Training ICT equipment, software and systems and a written declaration of understanding and adherence to this policy will be required in order to be provided access.

This policy cannot be viewed in isolation, and must be read in conjunction with the following documents and policies where appropriate:

- Keeping Children Safe in Education (DfE, 2021)
- The Prevent Duty – Counter-Terrorism and Security Act (2015)
- ATL Code of Conduct – Apprentices
- ATL Code of Conduct – Staff
- ATL Code of Conduct – Traineeships
- ATL IT Security policy
- ATL Loan Equipment policy
- ATL Monitoring and Logging policy
- ATL Prevent Action Plan
- ATL Privacy policy
- ATL Safeguarding policy
- ATL Training and Development policy
- ATL Whistleblowing policy

3. Impact on the Learner:

The implementation of this policy will help to ensure the safety and security of all learners, and other users, whilst using Aspiration Training ICT equipment, software and systems through providing clear and comprehensive information, guidance and support information. This includes protecting the learner, and all other users, from extremist views, the risk of radicalisation and being drawn in terrorism.

4. Definitions:

4.1 Aspiration Training ICT Equipment:

Any physical hardware, software of system provided by Aspiration Training for you to use. This includes any hardware, software or systems supplied by third party organisations, whether primary or secondary, irrespective of location. This may include, but not be limited to:

- E-Portfolio system
- Laptop / Desktop computer
- Management Information System (MIS) database
- Mobile / Smartphone
- Mobile storage devices
- Smart tablet

4.2 Cyber-Bullying:

Bullying can include a variety of behaviours from one individual / group to another individual / group such as name calling, offensive language, coercion, theft or damage, spreading harmful messages, hate crime or mate crime which is befriending someone with the intent to exploit them in some way. Cyber-bullying is when these behaviours take place using Information and Communication Technologies (ICT). Aspiration Training cyber-bullying as unacceptable and treats any allegation of this as seriously as any other type of bullying. If an allegation of cyber-bullying is sustained, it will be dealt with under the relevant disciplinary procedures and could result in removal from programme or dismissal. Please see appropriate Code of Conduct for further information.

4.3 E-Safety:

E-safety relates to the use of the internet, including the use of social media platforms, but also includes other electronic communications such as mobile / smartphones. Some people use these technologies to harm others or put them at risk of harm. Types of harm can range from sending hurtful or abusive messages and emails, to enticing children to radicalisation, exposure to terrorist organisation or engaging in sexual harmful conversations or actions online, webcam filming, photography, face-to-face meetings. It must be noted that harmful behaviours are not always perpetrated on younger people by adults, and can occur between people of a similar age. More information on this can be found in the ATL Safeguarding policy. Aspiration Training has a duty of care under the Prevent Duty (Counter-Terrorism and Security Act, 2015) to protect and inform all its learners and IT users regarding the risks and responsibilities of e-safety.

4.4 Phishing emails:

Phishing is the fraudulent practice of sending emails, often purporting to be from a reputable company, in order to convince recipients to reveal personal information such as passwords or bank card numbers, often with the intention of committing fraud or hacking. Further information relating to phishing and other types of cybercrime can be found on the Action Fraud website which is part of the National Fraud and Cyber Crime Reporting Centre.

5. Guidance and Procedures:

5.1 Acceptable Use of Email:

Anyone with a professional Aspiration Training email account has been provided with that email address because it is essential for them to conduct their professional duties properly and fully. Professional email accounts are for work-related communications and all Aspiration Training-related communications must be conducted via professional email accounts only.

All communications made using professional email accounts must relate to work-related duties and you must ensure the content and tone are professional at all times and are related to the subject of the communication. The level of professionalism and attention to detail should be equal to that of a formal letter.

Email should not be the preferred form of communication for confidential, personal or other sensitive information (eg learner or employer details, staff appraisals or any comments relating to job performance or disciplinary issues). Emails cannot be regarded as totally private and visible only to the intended recipient(s). As such, if emails are to be used to send personal or sensitive information or data, they must be encrypted and password-protected prior to sending.

Communications via professional email accounts may be monitored from time-to-time. Please note that all online activity must not bring an individual(s) in their professional role or Aspiration Training into disrepute.

Authorised ICT staff may access your professional email account if you are absent and there is Aspiration Training-related business information captured within the account which cannot be otherwise accessed and requires action before your anticipated return.

Aspiration Training recognises that you will be able to access personal email accounts on Aspiration Training equipment, and that it is reasonable for you to be able to do so, provided that you do not utilise your personal email account(s) for transmitting or storing Aspiration Training data and or personal and / or sensitive information. This requirement is to protect the integrity of Aspiration Training systems and data.

5.2 Acceptable Use of ICT Equipment:

Aspiration Training ICT equipment is provided to enable you to undertake your learning and / or professional duties. Such equipment must be treated and used in as careful and responsible way as it would be in the workplace.

You are expected to adhere to this policy when using all Aspiration Training equipment. This means that you remain liable for the use of the equipment and any and all associated passwords.

Aspiration Training ICT equipment may be used for the following:

- Teaching, learning and assessment activities
- To store data relating to Aspiration Training and its professional activities
- To run software or access systems supplied by Aspiration Training
- To load text, images, video or audio, subject to any copyright or licensing requirements, in connection with normal working requirements

5.3 Acceptable Use of the Internet:

Professional Use

The internet may be used to access relevant websites, including for the teaching, learning and assessment purposes. All online activity leaves a digital footprint that can be traced back to the relevant equipment, so please use Aspiration Training equipment responsibly.

Personal Use

Aspiration Training recognises that you may need to access the internet for non-work-related purposes using Aspiration Training ICT equipment. All online activity leaves a digital footprint that can be traced back to the relevant equipment, so please use Aspiration Training equipment responsibly.

Under no circumstances should you browse, download, upload or distribute any material that could be considered to be discriminatory, abusive, pornographic, obscene, harmful, illegal, offensive, discriminatory, potentially libellous or defamatory.

Personal use of social media, websites, blogs etc should make no reference to Aspiration Training, its learners or colleagues (except, in the case of colleagues, consent is obtained in advance), regardless of whether these sites are accessed whilst in the workplace or not. Any derogatory comment which explicitly or implicitly criticises Aspiration Training, its employees, learners or a related third party may lead to disciplinary action in addition to any claim for defamation.

Accessing Unlawful and / or Radicalising Material

Under no circumstances should you seek to access unlawful and / or radicalising material which promotes illegal / proscribed terrorist groups. A range of filtering software has been installed on Aspiration Training ICT equipment which both inhibits access to these sites and also produces reports of attempted access to these sites to the ICT team. These reports are shared with the Lead Designated Safeguarding Officer who will determine whether further action should be taken, in line obligations to the Prevent Duty and Counter-Terrorism and Security Act (2015), on an individual case by case basis. Regular checks will be made by the ICT staff team to ensure all filtering software is working effectively.

If you suspect that anyone using Aspiration Training ICT equipment to access illegal / proscribed material you should report it immediately using the process defined in the ATL Safeguarding policy.

5.4 Antivirus Protection:

You are required to take all reasonable steps to avoid the introduction of any virus to any Aspiration Training ICT equipment, systems or networks.

Reasonable steps include, but are not limited to:

- Not using any removable media, such as a memory stick, unless encrypted and with prior approval from a member of the ICT team
- Being cautious when opening any emails that you are not expecting, especially those which contain an attachment
- Not following any links to questionnaires, offers, requests etc from unknown sources. If these are received the email should be permanently deleted immediately.
- Forwarding suspicious email to the Helpdesk **only** and to no other recipient's email address
- Not installing any hardware or software without explicit written permission from a member of the Helpdesk team
- Ensuring any Aspiration Training ICT equipment provided for use off-site benefits from regular connection to the internet to enable anti-virus updates to be installed. This can be done either through using the device to log onto the relevant network(s) and allowing the updates to run or by allowing access to the device by a member of the ICT staff team, physically or remotely, so that required updates can be undertaken.
- Contacting the It Helpdesk team immediately for advice if you suspect that there may be a virus on any piece of Aspiration Training ICT equipment and stop using the piece of equipment until advised otherwise by a member of the ICT staff team
- Reporting any attempted phishing emails to the Helpdesk team so that they can ensure investigations are undertaken to determine the extent of other Aspiration Training IT Users affected. Often a phishing email is sent to several people.

5.5 Compliance with Legal and Statutory Obligations:

Aspiration Training is fully aware of its obligations within the following legal frameworks and is committed to meeting its legal requirements. Relevant legislation includes:

- Computer Misuse Act (1990)
- Copyright, Designs and Patents Act (1998)
- Counter-Terrorism and Security Act (2015)
- Data Protection Act (2018)

Aspiration Training will ensure compliance with the requirements any related future legislation.

5.6 Incident Reporting:

You should report any actual or attempted security breaches, loss of equipment or data to the Data Protection Officer (DPO) as soon as is practically possible. The details of the incident should be emailed to **both** dpo@aspirationtraining.com **and** helpdesk@chameleonsupport.co.uk.

If you have any concerns regarding phishing emails, unsolicited emails and any suspected or actual unauthorised or misuse of Aspiration Training ICT equipment, or have any other concerns relating to IT use, these should be reported to your Vocational Coach / line manager immediately.

In the event that you receive an email that you consider to be abusive through your professional email account, either from within Aspiration Training or from any third party, this should be reported to your Vocational Coach / line manager immediately.

If you have any concerns that Aspiration Training IT equipment is being used to threaten, intimidate, discriminate, harm, radicalise or pose any kind of threat to yourself or anyone else, you must report this immediately using the process identified in the ATL Safeguarding policy.

5.7 Password Security:

Secure and strong passwords are essential to protect the integrity of ICT systems and access to personal and / or sensitive data and information. The longer a password is, the more secure it is, for example a song lyric or memorable phrase plus a number eg *EducationcreatesInnovation007*. Do not choose a password which is so complex it is difficult to remember without writing it down. **Your password must not be disclosed to anyone else.**

Your password should be difficult to guess. For example, you could base your password on something that no-one else would know, eg the name of a favourite teacher from school. You should not use information which other people may know, or be able to find out, such as your address or date of birth.

You must not use a password which is used for another account. For example, you must not use the same password for both your private and professional Office 365 email accounts.

Passwords and any other security credential(s) you are issued with must be kept secure and confidential, and not shared be shared with, or given to, anyone else.

You must only use your own login and password when logging into Aspiration Training ICT systems. Passwords must be changed whenever there is a system prompt to do so or where there is a possibility that there might have been a possible compromise of the system or your password.

Where temporary passwords are issued to an individual, for any reason, they should be changed at first logon to a different, permanent password using the guidance above.

Passwords should not be written down.

Failure to comply with these requirements could lead to you compromising Aspiration Training's system security and would therefore be considered to be a breach of this policy.

5.8 Personal and Confidential Data:

All use of personal and confidential data must be in accordance with the Data Protection Act (2018). This applies equally whether in Aspiration Training premises, taken off Aspiration Training premises or accessed remotely.

You must ensure that personal data is kept secure used appropriately at all times.

To protect personal, sensitive, confidential or classified data, and to prevent unauthorised access to it, you will need to:

- Ensure screen displays of such data are always kept out of direct view of any individual who does not need to access that information as part of their role, and out of view of any third parties which includes online meeting or conferencing platforms such as Zoom or Microsoft Teams.
- Ensure screens are locked before moving away from your computer **at all times.**
- Ensure the logging off process for all pieces of ICT equipment is fully completed when you are going to be away from the device(s) for an extended period
- Personal data must always be stored within Aspiration Training equipment and systems and should only be accessed remotely by an appropriately authorised individual. Personal or sensitive data should not be emailed unless encrypted, and particular care must be taken when travelling by public transport both to ensure personal data is inadvertently viewed and to ensure that the ICT device is no left behind.

The security of Aspiration Training's systems will be reviewed regularly by members of the ICT staff team to ensure they are working effectively.

5.9 Safe Use of Images:

Images of learners and / or individuals may only be taken, stored and used for professional purposes in accordance with the law and with Aspiration Training policies. Particular regard must be given to the provision of written consent of the parent, carer or individual(s) depicted in the image(s) to the taking, storage and use of the image(s). Further information can be found in the ATL Privacy policy and Privacy Notices.

You are expected to support Aspiration Training's approach to online safety and not deliberately upload or add any images, video, sounds or text which may cause upset, distress or offence to any member of Aspiration Training or the wider community.

5.10 Teaching, Learning and Assessment:

The internet is used by Aspiration Training to raise standards in teaching, learning and assessment and to support the professional work of staff. We want to equip our learners with all the necessary ICT skills that they will need to progress confidently and competently in their chosen working environment and / or next level of education or training.

To achieve this effectively and safely:

- Cameras must be on for all learners throughout the duration of remote teaching, learning and assessment sessions. If the content of a particular session causes, or is liable to cause upset or distress, a learner should raise this with their Coach as soon as possible, either verbally or via the private chat function, and turn off their camera whilst the topic is under discussion. The learner should then turn their camera back on when the subject has finished, or agree to a post-session meeting with the Coach at the end of the session, ensuring their camera is switched on so that the Coach can be visibly reassured of their safety and wellbeing.

- Teaching, learning and assessment guidance must make reference to evaluating internet content for accuracy and intent. All learners will be encouraged and guided to be critically aware of the materials they access and how to validate information before it is accepted as being accurate.

- Learners are taught to acknowledge the source of any information used and to respect copyright. Learner handbooks will advise on referencing techniques and the seriousness of consequences if plagiarism is identified.

Under no circumstances should you browse, download, upload or distribute any material that could be considered to be discriminatory, abusive, pornographic, obscene, harmful, illegal, offensive, discriminatory, potentially libellous or defamatory.

Under no circumstances should you seek to access unlawful and / or radicalising material which promotes illegal / proscribed terrorist groups. A range of filtering software has been installed on Aspiration Training ICT equipment which both inhibits access to these sites and also produces reports of attempted access to these sites to the ICT team. These reports are shared with the Lead Designated Safeguarding Officer who will determine whether further action should be taken, in line obligations to the Prevent Duty and Counter-Terrorism and Security Act (2015), on an individual case by case basis. Regular checks will be made by the ICT staff team to ensure all filtering software is working effectively.

If you suspect that anyone using Aspiration Training ICT equipment to access illegal / proscribed material you should report it immediately using the process defined in the ATL Safeguarding policy.

6 Responsibilities:

6.1 Staff, Learners and Third-Party Aspiration Training ICT Users:

All staff and learners of Aspiration Training, associates, contracted agency staff, third-parties and collaborators on Aspiration Training projects will be users of Aspiration Training IT equipment, software and systems. All users must first be approved for use, and this carries with it the responsibility to abide by this policy and its principles and relevant legislation, supporting policies, procedures and guidance. No individual should be able to access information to which they do not have a legitimates access right. Although systems are in place to prevent this, no individual should knowingly contravene this policy or allow others to do so.

6.2 ICT Equipment, Systems and Software Owners:

Many Aspiration Training staff will have specific or overarching responsibilities for preserving Aspiration Training's intellectual property.

6.3 Systems Administrator:

Responsible for the information system, both manual and electronic, that supports Aspiration Training work. Responsibilities as above (for Principal Investigators / Project Administrators).

6.4 Information Security Manager:

Responsible for physical aspects of security and will provide specialist advice throughout Aspiration Training on physical security issues.

Responsible for the Acceptable Use of IT and e-Safety policy and subsequent security policies, and will provide specialist advice throughout Aspiration Training on information security issues.

6.5 Data Protection Officer:

Responsible for advising on and recommending information security policies to the GDPR steering group, assessing security risks, and identifying and implementing controls to identified risks. Responsible for approving information security policies to the GDPR steering group, assessing information security risks and identifying and implementing controls to risks.

Responsible for approving information security policies and acting upon any relevant guidance or issues raised by the above responsible staff.

7 Communication:

All staff, learners and third-party users of Aspiration Training ICT equipment will be made aware of this policy during their induction period and will be required to undertake a declaration of understanding and compliance with this policy and its requirements.

E-safety is integrated into teaching, learning and assessment opportunities as appropriate and as part of safeguarding content.

This policy is available on the Aspiration Training website to ensure access at all times, and may be provided in hard copy upon request. A Welsh version of this policy will be made available upon request.

8 Monitoring and review processes:

This policy will be reviewed on an annual basis, or when statutory guidance changes, to ensure it continues to meet the needs of the organisation and its stakeholders. The review will be validated by the Aspiration Training Board of Directors.

9 Contact details:

Data Protection Officer: dpo@aspirationtraining.com

IT Helpdesk: helpdesk@chameleonsupport.co.uk

Safeguarding Team: safeguarding@aspirationtraining.com

If you would like to discuss this policy further, please contact:

Wales	**England**
Neil Tamplin Managing Director, Aspiration Training Wales First Floor, Building Two, Eastern Business Park, St Mellons, Cardiff CF3 5EA Email: ntamplin@aspirationtraining.com Tel: 02921 175352	Mike Jones Managing Director, Aspiration Training England Fourth Floor, Grosvenor House, Prospect Hill, Redditch, B97 4DL Email: mjones@aspirationtraining.com Tel: 01527 359646