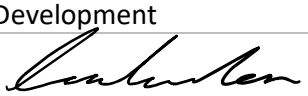
Policy title:	Online Safety and Social Media Policy		
Scope:	Achieve Training		
Policy owner & job title:	Hannah Warburton Head of Learner Wellbeing and Development		
Signed:		**Date:**	13.12.21
Approver:	Daniel Canavan		
Signed:		**Date:**	13.12.21
Date:	13.12.21	**Review Due Date:**	**13.12.22**

POLICY SUMMARY

Achieve Training's intent is to keep learners safe whilst acknowledging the benefits and opportunities which new technologies offer to teaching and learning.

We acknowledge that colleagues and learners have a right to use social media and online systems for their personal use but request that the guidelines of this policy are adhered to for the safety of all.

Achieve Training aims to take a whole organisation approach to online safety under the umbrella of our established safeguarding policies and procedures which support the identification and intervention of relevant concerns.

This policy outlines our approach to online safety, roles and responsibilities as well as defining the actions Achieve Training and our partner organisations will undertake to address any potential incidents or issues.

This policy will be reviewed on an annual basis or sooner should guidance/ legislation change.

ASSOCIATED POLICIES

Achieve Training's online safety policy runs in conjunction with the following legislation and policies:

- Keeping Children Safe in Education 2021
- Working Together to Safeguard Children 2018
- The Children Act 2004 as amended by the Children and Social Work Act 2017
- Relationships Education, Relationships and Sex Education, Health Education Guidance
- Safeguarding Policy and Procedure 2021
- Acceptable Behaviour Policy 2021
- Peer on Peer and Sexual Harassment/Violence Policy 2021

1. POLICY STATEMENT

The provisions and requirements of this policy apply to all learners, apprentices, and customers of Achieve Training. It is expected that all staff and customers use IT equipment for appropriate purposes through Achieve Training's systems and while undertaking activities related to Achieve Training.

This policy is intended to reinforce to all staff the importance of being aware of the potential safeguarding issues surrounding the use of ICT and social media and to advise of roles and responsibilities in relation to the safeguarding (online) of our learners, apprentices and other stakeholders.

To ensure our learners are kept safe, we will ensure that sufficiently experienced and competent individuals are involved in all areas of the organisation where there is any contact with learners, and that there is a designated safeguarding team and senior managers responsible for overseeing the implementation of this policy.

The Board of non-executive directors will undergo basic training; receive regular updates on safeguarding activities in addition to agreeing and reviewing policies. A designated board member assumes the role of Safeguarding Champion to assist and advise.

Online safety learning activities are embedded through the learning programmes through personal and social development curriculum to ensure awareness of online risks and how to keep safe online.

Achieve Training acknowledges our responsibilities in relation to The Prevent Duty 2015 in ensuring that our learners are safe from terrorist material when accessing the internet through the course of their learning and activities on programme.

All persons attending Achieve Training should be aware that Social Media sites may be used when investigating complaints and potential disciplinary matters such as cyber bullying and harassment.

Visiting any sites which could have a negative impact on Achieve Training or the welfare of colleagues or learners, is likely to be considered a disciplinary offence.

The use of the internet at Achieve Training is closely monitored and all users should be aware of possible implications when they utilise the internet access provided.

2. ONLINE SAFETY RISKS

Issues classified within the area of online safety can be categorised into four areas:

Content: being exposed to illegal, inappropriate or harmful content for example, fake news, racism, misogyny, pornography, anti-Semitism, radicalisation and extremism.

Contact: being subject to harmful online interaction with other users, for example; peer to peer pressure, commercial advertising, grooming for the purposes of sexual, criminal, financial or other purposes.

Conduct: personal online behaviour that increases the likelihood of, or causes harm, for example making sending or receiving explicit images and online bullying.

Commerce: risks such as online gambling, phising and /or financial scams.

3. FILTERING AND MONITORING

Achieve Training uses filtering systems installed on company devices monitored by our ICT department to ensure that access to inappropriate online content is limited by inaccessibility to sites by learners, apprentices, and staff.

Achieve Training are committed to reviewing the effectiveness of the current systems in place and where necessary, considering the implementation of further systems including relevant monitoring.

4. ROLES AND RESPONSIBILITIES

Roles and Responsibilities for online safety at Achieve Training:

- Overall Safeguarding Lead – Daniel Canavan (Executive Director of Achieve Training)
- Senior Manager- Hannah Warburton (Head of Learner Wellbeing and Development) -hannahw@achievetraining.org.uk
- Designated Safeguarding Manager -Sharon Francis- sharon@achievetraining.org.uk
- Safeguarding Board Champion – Elizabeth Shenton - who is regularly updated with an overview of all matters relating to Safeguarding.
- All staff are responsible for embedding and monitoring online safety of learners/apprentices under their supervision.

Achieve Training in execution of its duties to safeguard learners, apprentices and staff online, aims:

- To ensure all colleagues have a good understanding of online safety risks and acceptable social media use.

- To ensure all colleagues know what action to take in relation to online safety concerns.

- To ensure we make our learners aware of the potential dangers they face and how they can protect themselves.

- To ensure that all colleagues and learners use ICT systems, including accessing the internet and using mobile devices, in accordance with procedures and agreements.

- To ensure a process whereby colleagues agree to an internet usage policy during their induction before they are permitted to use any ICT systems at Achieve Training or within Aspire.

To fulfil our aims we will:

- Ensure Safeguarding Leads and Managers ensure that online safety is adhered to and issues dealt with accordingly and will:
    - Lead the monitoring and review of online safety policies / documents.
    - Ensure that colleagues are clear of procedures to raise online safety concerns through appropriate training and CPD opportunities
    - Liaise with the Local Authority in respect of Safeguarding and Prevent Policies
    - Liaise with ICT Technical colleagues on needs relating to online safety.
    - Report online safeguarding concerns along with other safeguarding data to SMT on a monthly basis and Board on a quarterly basis.

- Ensure our training centres are supported by ICT Technical staff through our IT Group Services department and that they will ensure:
    - That ICT infrastructure is secure and is not open to misuse or malicious attack
    - That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
    - Work with Safeguarding Leads and senior managers to support implementation of procedures and, software and systems to support online safety within the organisation.

- Ensure that teaching and support colleagues take responsibility for ensuring that:

- They have an up-to-date awareness of online safety and social media usage matters and of the current policy and practices.
- They report any suspected misuse or problem to the Safeguarding Manager for investigation.
- Digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official systems.
- Online safety issues are embedded in all aspects of the curriculum and other centre activities
- They monitor ICT activity in sessions.
- They are aware of online safety and social media usage issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current policies with regard to these devices.
- In sessions where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

- Ensure that learners:
    - Are responsible for using the systems in accordance with the Learner Acceptable Use and Technical Devices Agreement which they will be expected to sign at induction.
    - Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
    - Know and understand linked policies such as Acceptable Behaviour and Student Code of Conduct Policy, Safeguarding and Prevent Policies.
    - Understand the importance of adopting good online safety and Social Media usage, practice when using digital technologies out of the Achieve Training offices

- Ensure that all colleagues understand their responsibilities, as outlined in this policy. Training will be offered as follows:
    - A planned programme of CPD training related to online safety risks, these policies and the responsibilities it lays out will be made available to staff.
    - All new staff should receive an induction by our Group services ICT department as part of their induction programme, ensuring that they fully understand Achieve Training's online safety policy and the Acceptable Use and Technical Devices Agreement.

- Ensure that in learners sessions colleagues will reinforce the e-safety messages in the use of ICT by being aware and:
    - In lessons where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use

and that processes are in place for dealing with any unsuitable material that is found in internet searches
    - Where learners are allowed to freely search the internet, eg using search engines, staff should be vigilant in monitoring the content of the websites the learners visit
    - Learners should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
    - Learners should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

- Ensure that the use of digital and video images takes account of good online safety principles:
    - When using digital images, colleagues should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.
    - Colleagues obtain consent from parents / carers before any digital / video images are taken of any learner who is under the age of 18 (permission is not required in cases where a learner is over the age of 18) and only allowed to take digital / video images only to support educational aims. Those images should only be taken on Achieve Training equipment. A parental consent form is issued to parents/carers/guardians during induction, this covers the written permission from parents or carers obtained before photographs of learners are published on the Achieve Training website or used by the Aspire Group promotionally.
    - Care should be taken when taking digital / video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or Achieve Training into disrepute
    - Learners must not take, use, share, publish or distribute images of others without their permission.
    - Photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images
    - Learners' full names will not be used anywhere on a website or blog, particularly in association with photographs
    - Learners' work can only be published with their permission and where appropriate their parents or carers

- Ensure all users are aware of unsuitable and/or inappropriate activities:
    - Some internet activity e.g., anything that would be considered offensive or illegal would be banned from Achieve Training systems.

- Other activities e.g., Cyberbullying will be banned and could lead to criminal prosecution.
- As learners have their own mobile devices they are made aware of Achieve Training's policy on inappropriate usage which could be classed as bullying, cause offence or be considered illegal, regardless of the device that might be used in such actions
- There are however a range of activities which may, generally, be legal but would be inappropriate in an education or employment context, either because of the age of the users or the nature of those activities

5. CYBER BULLYING

Cyberbullying is any form of bullying which takes place online or through smartphones and tablets, on social networking sites, gaming platforms – through messages and or video.

Key points:

- Anyone who makes threats to on the internet could be committing a criminal offence. It's against the law in the UK to use the phone system, which includes the internet, to cause alarm or distress
- Keep safe by using unusual passwords. Use a combination of letters, lowercase, uppercase, symbols and numbers
- You can also report bullying to an organisation called Report Harmful Content online and they can help to get things taken down

Examples of bullying behaviour:

- Sending threatening or abusive text messages or e-mails, personally or anonymously
- Making insulting comments about someone on a website, social networking site (eg: Facebook, twitter etc.) or online diary (blog)
- Making or sharing offensive or embarrassing videos or photographs of someone via mobile phone or e-mail
- It should be noted that the use of ICT to bully is against the policy at Achieve Training and could be against the law
- Abusive language or images, used to bully, harass or threaten another, whether spoken or written (through electronic means) may be libellous, may contravene the Harassment Act 1997 or the Telecommunications Act 1984
- Bullying is based on unequal power relations, real or perceived. It will usually be repeated and be difficult to defend against. It is intended to hurt the bullied emotionally and/or physically
- "Bullying can be done verbally, in writing or images, including through communication technology (cyber bullying) e.g.: graffiti, text messaging, e-mail or postings on websites. It can be done physically, financially (including damage

to property) or through social isolation. Verbal bullying is the most common form.

6. PREVENT

Section 26(1) of the Counter Terrorism and Security Act 2015 places a duty on 'specified authorities' when exercising their function, to have due regard to the need to prevent people being drawn into terrorism.

As an Independent Training Provider, Achieve Training recognises this duty and responsibilities we have to safeguard our learners and apprentices in relation to this topic.

Achieve Training acknowledges that online activity can increase a young persons vulnerability to being groomed/ radicalised by extremist groups. The provisions and responsibilities of individuals set out in this policy and associated policies such as **Achieve Safeguarding Policy 2021** and, **Prevent Policy 2021** and **Acceptable Behaviour Policy 2021** aim to raise awareness of such risks to both staff and students and put measures in place to reduce the likelihood of such actions occurring.

7. EQUALITY AND DIVERSITY

This policy has been considered against our Equality and Diversity Policy and is designed to mitigate against potential direct or indirect discrimination.

APPENDIX A

If a bullying incident directed at a learner occurs using email or mobile phone technology:

- Advise the learner not to respond to the message
- Report to Safeguarding Leads
- Secure and preserve any evidence
- Inform the sender's e-mail service provider
- Notify parents of the learner involved
- Inform the local authority e-safety officer (where necessary)

If malicious or threatening comments are posted on an Internet site about a learner or member of staff you need to:

- Inform and request the comments be removed if the site is administered externally
- Secure and preserve any evidence
- Inform police as appropriate
- Inform LA e-safety officer (if appropriate and applicable)

If an incident involving a learner has occurred online and is of a sexual nature, staff must:

- Report to the Safeguarding Lead immediately (the safeguarding lead will follow appropriate safeguarding procedures and report to external agencies if necessary.
- Not request the learner to send related messages/images to the staff member but preserve these.

Learners should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

Useful links:

- http://www.ceop.gov.uk/
- http://www.childnet-int.org/