Policy title:	**E Safety and Social Media Policy**		
Scope:	Achieve training		
Policy owner & job title:	Hannah Warburton, Head of Learner Wellbeing and Development		
Approver:	Jason Lancaster, Training Operations Director		
Date:	31 July 2020	**Review Due Date:**	31/12/21 **Currently under review**

POLICY SUMMARY

'Keeping 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

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

1. POLICY STATEMENT

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.

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

- Keeping Children Safe in Education 2019
- Working Together to Safeguard Children 2018
- The Children Act 2004 as amended by the Children and Social Work Act 2017
- Safeguarding Policy 2020
- Safeguarding Procedure (Achieve Training) 2020
- Achieve Training Bullying and Harassment Policy (Part of Acceptable Behaviour Policy - Learners 2020)

Safeguarding legislation applies primarily to young people up to the age of 18. However, the provisions and requirements of this policy apply also 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 the importance to all colleagues at Achieve Training of being aware of the potential safeguarding issues and potential abuse & bullying surrounding young people and the safe and appropriate use of ICT and Social Media.

In order 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 are a number of Designated Safeguarding Officers.

As soon as learners start at Achieve Training they will be given advice and guidance on e-safety, social media bullying & harassment, appropriate use of website & online resources/systems and Prevent. They will also be assured that all colleagues will act immediately on any information about inappropriate behaviour or an individual's concerns. They will be asked to sign an Acceptable Use document to confirm their understanding.

Roles and Responsibilities for E Safety at Achieve Training:

- Safeguarding Lead – Jason Lancaster (Director of Training Operations) - jlancaster@achievetraining.org.uk
- Elizabeth Shenton - Safeguarding Champion – who is constantly updated with an overview of all matters relating to Safeguarding.
- Designated Safeguarding & E Safety/Social Media Officer/Coordinator – Hannah Warburton – hannahw@achievetraining.org.uk
- Head of Learner Wellbeing and Development responsible for on-line safety of all young people at training centres.
- Learner Services colleagues responsible for e-safety education of all young people at their centre.
- Tutors and Assessors are responsible for monitoring, and e-safety education within their lessons and support sessions and for reinforcing e safety education.

E-safety and Social Media Use

Aim:

- To ensure all colleagues have a good understanding of e-safety and acceptable social media use, in particular the types of dangers learners may face:
- To ensure all colleagues know what to do in the event of an e-safety incident
- 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. All

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.

Learners attending Achieve Training are asked to respect that centres are run as any other workplace. This means that mobile phone use is not accepted in workshops or classrooms by either learners or colleagues. Many classrooms have mobile phone lockers where they can be stored during lessons.

Potential Dangers

The development and expansion of the use of ICT, particularly of the internet, social media sites and mobile devices, has transformed learning in recent years. Young people need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. Learners will be made aware of their obligation not to use Social Media to make defamatory comments about their employers and their place of work.

There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning. The benefits are perceived to "outweigh the risks." However, at Achieve Training, through our e-safety policy, we ensure that we meet the statutory obligations to ensure that young people are safe and are protected from potential harm by understanding consequences of misuse.

As progress is made to introduce other learning platforms, Achieve Training will ensure that there is full awareness of usage and security, specific guidance will be given to all.

However, the use of these new technologies can put young people at risk within and outside Achieve Training centres. Some of the dangers they need to be aware of include:

- Access to illegal, harmful or inappropriate images or other content on websites
- Unauthorised access to, loss of, sharing of, personal information
- The risk of being subject to grooming by those with whom they make contact on the internet, through social media sites and on mobile devices, both within the context of Safeguarding and Prevent
- The sharing/distribution of personal images with or without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying and discrimination
- Access to unsuitable video/internet games/films
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music, video files or other content

- Sending offensive messages which with may offend or cause damage to persons or companies
- Disclosing confidential/personal information
- Access to gambling arenas that are not age appropriate and may result in consequences that may affect a young person in the long term
- The potential for excessive use, which may impact on the social and emotional development and learning of the young person
- The risks to their employment if they choose to use social media when absent from work due to illness and then declaring they are involved in social activities instead.

As with all other risks, it is impossible to eliminate them completely. We will therefore, through good educational provision, build learners' understanding of the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. They also need to be aware of the possible legal implications of their online activities.

To fulfil our aims we will:

- Ensure Achieve Training has an appointed E-Safety/Social Media Co-ordinator who will ensure that e-safety is adhered to and issues dealt with accordingly and will:
    - Take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing e-safety policies / documents
    - Ensure that all colleagues are aware of the procedures that need to be followed in the event of an e-safety incident taking place
    - Provide training and advice for colleagues
    - Liaise with the Local Authority in respect of Safeguarding and Prevent Policies
    - Liaise with ICT Technical colleagues
    - Receive reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
    - Meet regularly with training centre team members to discuss current issues, review incident logs and change control measures.
    - Report regularly to the Executive Team 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 users may only access the networks through a properly enforced password protection policy, in which passwords are regularly changed
    - 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

- That the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation

- Ensure that teaching and support colleagues take responsibility for ensuring that:
    - They have an up to date awareness of e-safety and social media usage matters and of the current e-safety policy and practices
    - They report any suspected misuse or problem to the E-Safety Co-ordinator 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
    - E-safety issues are embedded in all aspects of the curriculum and other centre activities
    - They monitor ICT activity in sessions, extracurricular and lunch breaks
    - They are aware of e-safety and social media usage issues related to the use of mobile phones, cameras and hand held 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 Policy, which they will be expected to sign before being given access to systems
    - Have a good understanding of research skills and the need to uphold copyright regulations
    - Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
    - Know and understand policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand policies on the taking / use of images and on cyber-bullying
    - Understand the importance of adopting good e-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 e-safety training will be made available to staff

- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand Achieve Training's e-safety policy and the Learner Acceptable Use Policy
- This E-Safety policy and its updates will be presented to and discussed by staff in team meetings
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required

- 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 e-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. In particular, they should recognise the risks attached to publishing their own images on the internet eg. 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 eg anything that would be considered offensive or illegal would be banned from Achieve Training systems.
  - Other activities eg 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

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.

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images
- Promotion or conduct of illegal acts, eg under child protection, obscenity, computer misuse and fraud legislation
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist material in UK
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Activity likely to support extremism or radicalisation as defined in the Achieve Training Prevent policy
- Threatening behaviour, including promotion of physical violence or mental harm

Cyber bullying is bullying through the use of communication technology e.g. mobile phone text messages, social media sites, twitter, e-mails or websites. This can take many forms for example:

- 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.

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

- Advise the learner not to respond to the message
- Refer to relevant policies including e-safety/ Social Media acceptable use, and the Bullying and Harassment policy
- Report to E-Safety coordinator
- 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
- Send all the evidence to COPD (Child Exploitation and Online Protection Centre part of NCA national Crime Agency)
- Endeavour to trace the origin and inform police as appropriate
- Inform LA e-safety officer

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/

2. 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.

3. RESPONSIBILITIES OF COLLEAGUES

All Achieve Training colleagues must ensure that they follow the processes for ensuring learners are safe when using ICT and social media platforms, websites, other online resources and that any and all e-safety concerns are reported as described in the policy.

All Achieve Training colleagues must ensure that they follow the guidelines outlined in the policy for conduct, behaviour and interaction with our learners.

4. RESPONSIBILITY OF ACHIEVE TRAINING

To ensure that training is available for all colleagues who have a direct responsibility for supporting learners to ensure they meet the requirements laid out in the statutory legislation and described in the policy.

To ensure that the policy is reviewed and updated at least annually to reflect changes to legislation and recommended practices by governing bodies such as OFSTED, ESFA, and local authorities.