Social Media, Staying Safe Online and Cyber Bullying Policy

1. Purpose of Policy

1.1 GEM Partnership places safeguarding at the heart of all that we do; we recognise the wide-ranging aspects of the term. GEM Safeguarding policies cover Safeguarding, Prevent and Equal Opportunities. This policy forms part of GEM's Safeguarding strategy and aims to support Staff and Learners in the use of IT and Online activities.

1.2 The aims of this policy and its supporting policies (email, telephone and social media) are to:

1.2.1 Set out the key principles expected of all members of GEM with respect to the use of digital technologies.

1.2.2 Safeguard and protect and educate the learners, candidates and staff.

1.2.3 Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.

1.2.4 Ensure that all members of the GEM are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

1.2.5 Set out definitions of Cyber Bullying and risks involved.

1.2.6 Define clear structures and processes to deal with inappropriate/illegal activity whilst using digital technology (noting that these need to be cross referenced with other policies).

1.2.7 Minimise the risk of misplaced or malicious allegations made against adults who work with students.

2. Key Advice for Staying Safe Online

2.1 How to stay safe online

2.1.1 Internet safety tips:

2.1.1.1 Never give out your real name

2.1.1.2 Never tell anyone where you live or work

2.1.1.3 Never give out your address or telephone number

2.1.1.4 Never agree to meet anyone from a chatroom on your own

2.1.1.5 Tell a manager if someone makes inappropriate suggestions to you or makes you feel uncomfortable online

2.1.2 Danger signs:

2.1.2.1 If the person tries to insist on having your address or phone number

2.1.2.2 If the person emails you pictures which make you feel uncomfortable and which you would not want to show to anyone else

2.1.2.3 If the person wants to keep their chats with you secret

2.1.2.4 If the person tells you that you will get into trouble if you tell a manager what has been going on

2.1.2.5 If the person emails you pictures which make you feel uncomfortable and which you would not want to show to anyone else

2.1.2.6 If the person wants you to email them pictures of yourself or use a webcam in a way which makes you feel uncomfortable

2.1.2.7 If the person shares information with you and tells you not to tell anyone else about it

2.1.2.8 If the person wants to meet you and tells you not to let anyone know

3. Roles and Responsibilities

3.1 GEM has a duty of care for ensuring the safety (including e-safety), the Safeguarding Lead – Julie Hunter and Safeguarding Officer – Kelly Lee are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see below).

3.2 All staff at all levels are responsible for ensuring that they have an up to date awareness of online safety matters and of the current policies and practices; staff are expected to follow policies on IT and Communications, Social Media and Data Protection, available in the Employment Policies Handbook.

3.3 Staff must report any suspected misuse or problem to the Safeguarding Lead or Officer and ensure all of their digital communications with students and colleagues should be on a professional level.

4. Use of Technology

4.1 Clear guidance on the use of technology for all users, including staff, learners and visitors that references permissions/restrictions and agreed sanctions is found in the following documents, which should be read in conjunction with this policy:

4.1.1 Data Protection Policy & Procedure.

4.1.2 Computer Facilities Policy

4.1.3 Staying Safe Online & Cyber Bullying Policy

4.1.4 Electronic Communication Policy

5. Social Media & Networking Sites

5.1 The Company respects your right to a private life and therefore you may access social networking sites using the Facilities. However, this should be done outside office hours and be kept to a reasonable limit. If there is any evidence that this privilege is being abused then the privilege may be withdrawn.

5.2 Your use of Social Networking sites may impact on the Company and its business. Such impact includes potentially causing damage to its reputation, loss of Confidential Information, or exposure to other liabilities such as claims of discrimination, harassment or workplace bullying. The content of any communications or comments posted on a Social Networking site must not damage or bring into disrepute the Company, its staff, clients or candidates. Therefore, if you use Social Networking sites, even where this is not via the Facilities or is outside of working hours you are prohibited from:

5.2.1 Engaging in any conduct or posting any comments which are detrimental to the Company.

5.2.2 Engaging in any conduct or posting any comments which could damage working relationships between members of staff, Introducers, suppliers, affiliates, Clients and Candidates of the Company. Where you express personal views, you must state that these are personal views and do not represent the views of the Company.

5.2.3 Engaging in any conduct or posting any comments which could be derogatory to another person or third party or which could constitute unlawful discrimination or harassment.

5.2.4 Recording any Confidential Information regarding the Company on any social networking site or posting comments about any Company related topics such as the Company's performance.

5.2.5 Making information available which could provide any person with unauthorised access to the Company, the Facilities and/or any Confidential Information.

5.3 You may be required to remove postings deemed to constitute a breach of this policy. This may include any 'likes' or 'dislikes' of other people's posts or the re-posting/tweeting of other people's comments which of themselves may constitute a breach of this policy.

5.4 Post termination of employment or engagement restrictions: For the avoidance of doubt, the restrictions on the use of Networking Sites continue to apply throughout Your employment with the Company including any period of garden leave you may serve.

6. Use of Social Media in Training

6.1 GEM supports the use of social media communication in training to support learners, employees and staff. A platform to express views, queries and feedback is essential to successful learning and development during a long programme of learning such as Apprenticeships.

6.2 GEM utilises and provides Social media groups to facilitate and promote communication channels within Apprenticeships. GEM have in place robust management of all social media activity in relation to learning and development activities. The lead Safeguarding Officer will monitor and deliver advice and guidance to staff on all Social media platforms.

6.3 GEM will monitor and report breaches to this policy, in relation to Cyber bullying, attempts to promote Radicalisation or Extremism, published content meets the high standard expect from GEM and identify Equality and Diversity trends and breaches in regards to the protected conditions.

6.4 GEM will provide advice and guidance to Learners and Staff through IAG induction activities and also in the Learner handbook.

6.5 GEM will promote British values, safeguarding and prevent information through the use of the Learner voice social media platforms and encourage discussion throughout the community. Breaches to this policy will be removed and reported to the appropriate authority.

6.6 GEM will provide Social media platforms through a closed group system and membership must be authorised by the compliance department, before access is granted. Any unauthorised membership or access will be removed.

6.7 Social media it a vital tool to aid the delivery of training and development, whist providing a platform for the learner's voice to raise concerns, issues or queries about learning. The use of online content and websites must be monitored and concerns reported. It is the responsibility of all GEM Staff to ensure learners and colleagues are kept safe at all times.

7. Cyber Bullying

7.1 What is cyber bullying?

7.1.1 Cyber bullying is any form of bullying which takes place online or through smartphones and tablets. Social networking sites, messaging apps, gaming sites and chat rooms such as Facebook, XBox Live, Instagram, YouTube, Snapchat and other chat rooms can be great fun and a positive experience if used in the way the site is intended. Cyber bullying is rife on the internet and most people will experience it or see it at some time. Cyber bullying can happen 24 hours a day, 7 days a week and it can go viral very fast.

7.1.2 Cyber bullying affects people from any age or walk of life, including children, teens and adults who all feel very distressed and alone when being bullied online. Cyber bullying can make you feel totally overwhelmed which can result in feeling embarrassed that they are going through such a devastating time, and not knowing what support is available to them. Many people feel uncomfortable to confide in someone they can because they feel ashamed and wonder whether they will be judged, being told to ignore it or close their account which they might not want to do.

7.2 Definitions of Cyber Bullying Types

7.2.1 There are many ways of bullying someone online and for some it can take shape in more ways than one:

7.2.1.1 Harassment - This is the act of sending offensive, rude, and insulting messages and being abusive. Nasty or humiliating comments on posts, photos and in chat rooms.

7.2.1.2 Denigration – This is when someone may send information about another person that is fake, damaging and untrue. Sharing photos of someone for the purpose to ridicule, spreading fake rumours and gossip.

7.2.1.3 Flaming – This is when someone is purposely using really extreme and offensive language and getting into online arguments and fights.

7.2.1.4 Impersonation – This is when someone will hack into someone's email or social networking account and use the person's online identity to send or post vicious or embarrassing material to/about others.

7.2.1.5 Outing and Trickery – This is when someone may share personal information about another or trick someone into revealing secrets and forward it to others.

7.2.1.6 Cyber Stalking – This is the act of repeatedly sending messages that include threats of harm, harassment, intimidating messages, or engaging in other online activities that make a person afraid for his or her safety.

7.2.1.7 Exclusion – This is when others intentionally leave someone out of a group such as group messages, online apps, gaming sites and other online engagement.

7.2.1.8 Threatening behaviour - Anyone who makes threats to you 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. It could also be against the 1997 Harassment Act.

7.2.1.9 Blackmail and grooming - online talking to someone who become a new "friend", who has tried to pressure you into taking their clothes off and filming or taking images of themselves. This is an offence called "grooming" in the UK. Everyone you meet on the internet is a stranger and you need to keep personal things personal to you, don't share your secrets with other people and if anyone asks you to do anything that makes you feel uncomfortable then don't do it.

8. Responsibilities of Users

8.1 Do not post abuse about anyone else online or send threats that may cause harm to you or the company reputation. Use of company equipment to do this will results in disciplinary action.

8.2 Keep safe by using unusual passwords. Use a combination of letters, lowercase, uppercase, symbols and numbers. Don't use any part of your name or email address and don't use your birth date either because that's easy for people who know you to guess. Don't let anyone see you signing in and if they do, change the password as soon as you can. Refer to Computer Facilities Policy.

8.3 If you are using a public computer such as one in a library, computer shop, or even a shared family computer, be sure to sign out of any web service you are using before leaving the computer so that you can protect your privacy. Refer to Staying Safe Online Policy.

8.4 If posting online for work purposes consider the content of the post to ensure no harm can be caused to the readers.

8.5 Don't post anything on a social networking site which gives your real name, address, school, phone number or which will allow a stranger to contact you in real life.

8.6 Don't upload anything that might embarrass you or the company at the time or at a later date.

8.7 If you have a webcam or smartphone never be pressured into taking pictures of yourself that you wouldn't want other people to see.

9. Effects of cyber bullying

9.1 What can you do to support someone who is being bullied online?

9.1.1 Reinforce that no one deserves to be treated in this way and that they have done nothing wrong

9.1.2 Ensure that they know that there is help available to them

9.1.3 Encourage them to talk to a manager that they trust

9.1.4 Take screen shots of the cyber bullying so that they have proof this is happening

9.1.5 Report all abuse to the relevant social media networks by clicking on the "report abuse" button

9.1.6 Keep a diary so they have somewhere safe and private to write down their innermost thoughts and feelings which will help to avoid feelings bottling up

9.1.7 Give praise for being so brave and talking things through which will hopefully empower them to take responsibility and get help

9.1.8 Sending abuse by email or posting it into a web board can be harassment and if this has happened make a complaint to the police who can trace IP addresses etc.

9.1.9 Involve the police if you feel nothing is being done to stop this bullying

9.1.10 If the cyber bullying is done by work colleagues, involve your HR Department so they are aware of what is going on, and give them copies of the screenshots. Ask them to put this on your personnel file.

9.1.11 You have the option of blocking the people that are cyber bullying you but this obviously doesn't stop it from continuing.

10. Company's Responsibilities

10.1 Ensure full training is given to users on awareness of Cyber Bulling

10.2 Monitor user use of computer facilities including internet. Refer to Computer Facilities policy.

11. Professional Development

11.1 All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the GEM Partnership's IT Security Policy and supporting policies and procedures.

11.2 All Staff must be aware of training requirements and will conduct Online safety training as part of their Continuous Professional Development.

12. Online Safety in the Apprenticeships

12.1 Online safety should be a focus in all areas of the curriculum. Staff reinforce online safety messages through their teaching and in pastoral contact, to promote responsible and resilient use of digital technologies by students and ensure they are well placed to protect themselves.

12.2 Apprentices are taught in all lessons to be critically aware of the materials they access on-line and be guided to validate the accuracy of information. They are also taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

13. Reporting Online Abuse/Misuse

13.1 Discovery of unsuitable use or materials, where no illegality is identified or suspected should be reported to your line manager and GEM Lead Safeguarding Officer who will work with the Directors other agencies to investigate, decide on a course of action and recommend/apply sanctions where necessary. In the event of the incident relating to a member of staff this will be referred to the HR Department.

13.2 Where illegal materials or activities are found or suspected this should be reported to the Designated Safeguarding Officer, if relating to Learners or Safeguarding, or Staff, the former will then be handled in compliance with the Safeguarding policy and procedures. The latter will be reported to the HR Department and subsequent steps will be determined by their response and in conjunction with the GEM's disciplinary policies and procedures. If the illegality pertains to a Safeguarding issue involving a member of staff it should be reported to the Operations Manager.

14. Support to Employers

14.1 GEM recognises that some employers have a limited understanding of online safety risks and issues, yet they play an essential role in the education of their employees and in the monitoring and regulation of their employee's on-line behaviours. Employers may underestimate how often employees come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

14.2 GEM therefore seeks to provide information and awareness to Employers through Information, Advice and Guidance publications and regular newsletter, the promotion of high-profile campaigns such as Safer Internet Day, as well as reference to relevant web sites and publications.

15. Status of this policy

15.1 This policy does not constitute a contract and the Company reserves the right to change its terms at any time. Failure to comply with this policy may lead to disciplinary action up to and including termination of your employment or engagement with the Company.

16. Related Policies

16.1 Staff should refer to the following policies that are related to this information security policy:

16.1.1 Data Protection Policy & Procedure.

16.1.2 Computer Facilities Policy

16.1.3 Information Technology Security Policy

16.1.4 Electronic Communication Policy