Bottle Green Training Ltd (BGT)   Online Safety and Social Networking Policy

Review and revision dates.

Effective from:	Version	Description
September 2021	1.0	Policy original
September 2022	1.0	Annual update: No amendments needed
March 2023	1.1	Re-branding
June 2023	1.1	Update: in line with KCSIE 2023
September 2023	1.1	Annual update: No amendments needed
September 2024	1.2	Annual update: Extra guidance added to staying safe online
December 2024	1.3	Update: Wording change: 'Staff are required to comply' changed to 'Staff must comply

Review Date:	September 2025 or as legislation requires
Published:	College notice board, Website, Learner handbook
Actions:	All updated policies will be emailed to the employees.
Company Directors Signatures:	

BGT ONLINE SAFETY AND SOCIAL NETWORKING POLICY

Policy aims.

To ensure, through safeguarding protocols and practices, that potential risks to staff and learners from social networking and online use are minimised.
To promote a professional working environment where staff and learners understand the parameters surrounding acceptable behaviour regarding the use of social media, company internet and company mobile phones.

Principles underpinning the Policy.

- BGT understand that electronic means of communication both in a professional capacity (office computers, mobile phones, Facebook, Internet, etc.), and the private capacity of staff and learners is part of the environment we live in.
- The online world offers a wealth of opportunities but can also present risks and challenges.
- The use of social networking sites and inappropriate usage of the internet introduces a range of potential safeguarding risks to learners and staff alike.
- BGT has a duty to ensure that all young people and adults involved in our organisation are protected from potential harm online whether they are using our network and devices.
- BGT in collaboration with our IT consultants will maintain and check the effectiveness of filtering and monitoring systems onsite.
- BGT recognise the four key areas of risk within online safety: Content – being exposed to illegal, inappropriate or harmful content, Contact – being subjected to inappropriate or harmful online interaction, Conduct – behaving in a manner that increases the likelihood of being exposed to or causing harm and Commerce – the risks of online gambling, phishing, inappropriate advertising or financial scams. We will provide advice and guidance to help apprentices/learners protect themselves from these harms.
- BGT recognises that technology and its applications are evolving at a fast pace and therefore this policy will be review and update at least annually to reflect significant changes in the social media environment.

Related BGT policies

- Learner behaviour
- Staff code of conduct
- Safeguarding and Prevent

Strategic implementation of the policy

- BGT will provide learners with clear guidance on how to behave online. This will be outlined during programme induction and within the learner code of conduct.
- All staff must co-operate, conform, and comply with the requirements of this policy and work with learners to develop their understanding and compliance.
- Staff will have received appropriate safeguarding training to understand the implications and potential adverse consequences of inappropriate use of both equipment used professionally and privately.
- Staff will have received PREVENT training to understand their duty in the Counterterrorism and Security Act 2015
- Staff will adhere to the Staff Code of Conduct in all matters regarding sharing of social media communications with learners and others and understand that should they compromise the safety of themselves or the company's integrity they will be subject to BGT disciplinary procedures.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation

Staying safe online

- Accept personal responsibility for your actions when using the internet, including social media platforms, games, and apps. This includes the resources you access and the language you use.
- Do not deliberately browse, download, or upload material that could be deemed offensive or illegal. If you accidentally come across any such material, report it immediately to your tutor or BGT centre manager.
- Do not send anyone material that could be considered threatening, bullying, offensive or illegal.
- Do not give out any personal information online, such as your name, phone number or address.
- Be vigilant! Especially when you receive emails to do with finance, security, or requests.

- Emails that request urgent action are designed to try and stop you thinking, instead focusing on a made-up deadline. Always question when a response or action is required in an immediate or unusual timescale.

- Always check the email address of the sender with the display name and the email body. If you see any spelling mistakes or errors in the address, it is most likely malicious. Remember a display name can be set to anyone's name.

- Think before clicking on any link that appears in an email. They can be setup to mask the malicious link. Only click on links if you know the sender and trust that the email looks legitimate, and that you are expecting this email with a link.

- Take care when using AI for research. This can blur the lines for plagiarism and many companies have built an industry on stealing IP addresses and black mailing users.

- When using social media be aware that it is public, and you are only as safe as all your friend's privacy settings.

- Take care to only allow people you want to see your location on your social platforms.

- Do not reveal your passwords to anyone.
- If you are concerned or upset about anything you see on the internet or any messages that you receive, report it immediately to your tutor, liaison officer or BGT centre manager.