

The following statement outlines SSG's stance on E-safety and the roles that are expected by Staff and customers/candidates/delegates. Failure to comply with the stated guidance will result in investigation to the nature of the activity around technology involved and the outcome, and may result in disciplinary action.

The main purpose of the E-safety policy is to safeguard staff and customers/candidates/delegates whilst engaging with digital technologies/media within the supervision of SSG.

Staff will have access to CPD training internally to promote awareness and improve confidence around E-safety.

Staff are responsible for ensuring that ...

- they have an up to date awareness of e-safety matters and of the current e-safety policy and practices
- they have read and understood the Acceptable Use Policy
- they report any suspected misuse or problem to their line manager for investigation and follow up action (if required)
- all digital communications with customers/learners/candidates/organisations should be on a professional level and only carried out using official SSG systems
- e-safety issues are embedded in all aspects of delivery and non-contact tasks
- customers/candidates/delegates understand and follow the e-safety and acceptable use policy
- customers/candidates/delegates have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in sessions and other activities (where allowed) and implement current policies with regard to these devices
- in sessions where internet use is pre-planned customers/candidates/delegates 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.

Customers/learners/delegates are responsible for ensuring that...

- they are using the company digital technology systems in accordance with the Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of SSG and realise that SSG's E-Safety Policy covers their actions away from SSG, if related to their association to the company.

Staff or customers/candidates/delegates who may have concerns, queries or questions regarding the above statement must speak with their direct line manager, failing this contact the Designated Safeguarding Lead.