E-Safety Policy

Background

Hughes Driver Training Ltd recognises the benefits and opportunities which modern technologies offer to teaching and learning. We provide internet access to all learners attending our courses and staff encourage the use of technologies, to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the company while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance, and implementation of our policies. In continuation of our duty to safeguard learners we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care.

The policy applies to all users, learners, and staff of Hughes Driver Training Ltd who have access to our IT systems, both on the premises and remotely. Any user of Hughes Driver Training Ltd IT systems must adhere to this policy. The E-Safety Policy applies to all who use the internet and forms of electronic communication such as email, mobile phones, and social media sites.

Role and Responsibilities

There are clear lines of responsibility for e-safety within the company. The first point of contact should be Head of Quality and Compliance. All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager. All tutors and assessors are required to offer guidance on e-safety to their learners and to read and report incidents in line with the policy. When informed about an e-safety incident, staff members must take care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved. All learners must know what to do if they have e-safety concerns and to whom to talk. In most cases, this will be the Head of Quality and Compliance. All parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, the Safeguarding Officer may be asked to intervene with appropriate additional support from external agencies.

E-Safety Officer / Safeguarding Officer:

The Safeguarding Officer is responsible for keeping up to date with modern technologies and their use, as well as attending relevant training. They will be

expected to complete, review, and update the E-Safety Policy, deliver staff development and training, record incidents, report developments and incidents to the SMT and consult with the local authority and external agencies to promote e-safety.

Learner:

Learners are responsible for using Hughes Driver Training Ltd IT systems and mobile devices in accordance with the company requirements. Learners must act safely and responsibly always when using the internet and/or mobile technologies. They are responsible for attending e-safety lessons as part of the curriculum and are expected to know and act in line with other relevant company policies e.g. mobile phone use, sharing images, cyber-bullying etc. They must follow reporting procedures where they are worried or concerned, or where they believe an e-safety incident has taken place involving them or another member of the company.

Staff:

All staff are responsible for using Hughes Driver Training Ltd IT systems and mobile services in accordance with company policies. Staff are responsible for attending staff training on e-safety and displaying a model example to learners always through embedded good practice. All digital communications with learners must be professional always. All staff should apply relevant company policies and understand the safeguarding incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to the Designated Safeguarding Officer and/or line manager without delay.

Security:

The company will do all that it can to make sure the company network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, workstations etc to prevent accidental or malicious access of company systems and information. Digital communications, including email and internet postings, over the company network, will be monitored in line with IT policies.

Behaviour:

Hughes Driver Training Ltd will ensure that all users of technologies adhere to the standard of behaviour as set out in IT policies. The company will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful always. Any reported incident of

bullying or harassment or any other unacceptable conduct will be treated seriously and in line with company and staff disciplinary codes.

Where conduct is found to be unacceptable, the company will deal with the matter internally. Where conduct is considered illegal, the company will report the matter to the police.

Personal Information:

Personal information is information about a living person that Hughes Driver Training Ltd collects and stores the personal information of learners and staff regularly e.g. names, dates of birth, email addresses etc. The company will keep that information safe and secure and will not pass this on without the express permission of the learner/parent/carer. No personal information can be posted on the company website without permission of the designated safeguarding officer unless it is in line with our data protection / GDPR policy.

Staff must keep learners' personal information safe and secure always. No personal data is permitted off site unless permission has been granted by the designated safeguarding officer. Where personal data is no longer required, it must be securely deleted in line with the Data Protection / GDPR policy.

Incidents:

Where an e-safety incident is reported to the company this matter will be dealt with. The company will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to their tutor or to the company Designated Safeguarding Officer. Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible. Following any incident, the company will review what has happened and decide on the most appropriate and proportionate course of actions. Sanctions may be put in place, external agencies may be involved, or the matter may be resolved internally depending on the seriousness of the incident.