**Online Safety Policy**

1. Introduction

1.1 Education and Skills understands its responsibility to educate its participants in relation to Online Safety issues in accordance with the online safety act 2023. The organisation is committed to ensuring that the programme conducts its operations in such a way that participants are equipped with the appropriate skills, behaviours and critical thinking skills to enable them to remain safe and act legally when using the internet and related technologies in any context or circumstances.

2. Objectives

2.1 Policy Objectives:

* To protect the interests and safety of Education and Skills learners
* To ensure that all employees and participants adhere to the IT usage rules to prevent any viewing or downloading of unsuitable material such as pornography, extremism, terrorism and anti - British web sites.
* To prevent unauthorised access to / loss of / sharing of personal information
* Prevent the risk of being subject to grooming by those with whom they make contact on the internet
* To ensure learners are aware of the risk of sharing / distribution of personal images without an individual’s consent or knowledge including images of ‘Upskirting’ (Voyeurism Offences Act 2019)
* To protect learners from cyber bulling

3. Responsibilities

3.1 Education and Skills strives to ensure that all participants are adequately safeguarded from potential security threats and misuse. It is critical therefore that all employees and participants comply with this policy and support its objectives.

3.2 The Designated Safeguarding officer James Hart and deputies Steve Martin and Nicola Williams will ensure that policy and safe practices are embedded in operations and activities and that team members receive suitable CPD to enable them to carry out their Online Safety roles and responsibilities.

3.3 The designated officers will ensure that participants receive regular, meaningful Online Safety education. Such activities will be provided in the following ways:

• Educating all participants on the dangers of technologies that may be encountered; including cyber bullying, radicalisation and staff must be aware of reporting procedures and prevent duty.

• Making participants aware of where and how to seek help if they experience problems when using the internet and related technologies

• Encouraging participants to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside work and the Apprenticeship programme

• Providing advice, guidance and information on safe, legal and acceptable internet use

• Detailing the effective and safe use of the internet in research, including the skills of: knowledge, location, retrieval and evaluation.

3.4 Both company directors will ensure that the ICT infrastructure is safe and not open to misuse or attack.

4. Employees

4.1 All employees are responsible for ensuring that all digital communications with participants are on a professional level only and that ICT usage and activities are monitored in activities including: classroom-based delivery, workshops and learning events. All Staff are given an education and skills email account and secure access to OneFile. These are to be used when contacting learner, and no personal contact information should be given out to safeguard all staff and learners.

5. Participants

5.1 All participants will receive Online Safety information, advice and guidance as part of their training with the use of side by side training modules.

5.2 It is crucial that participants understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so. Specific guidance is therefore provided at induction and information of the contact details for designated officers is on their OneFile account.

6. Blogging & Social Networking

6.1 Blogging is defined as writing a personal online journal that is frequently updated and intended for general public consumption. Social networking is defined as sharing your interests, information and emotions in an online forum with other employees. Common social networking sites include but are not limited to Facebook, YouTube, LinkedIn, Twitter, snapchat and TicToc. Social networking also can take place on online gaming platforms such as Roblox and Fortnight.

6.2 Blogging by employees and participants, whether using the company’s property and systems or personal computer systems, is subject to the terms and restrictions set out in this policy.

6.3 Employees and participants should not under any circumstances use the company’s systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog for non-business-related reasons, even in their own time.

6.4 Employees and participants should not, under any circumstances, use Education and Skills systems to access or participate in any social networking sites for non-business-related reasons during work hours. However, subject to compliance with the terms of this policy on acceptable use, access may be granted to certain sites which individuals may be able to access for work or learning purposes. However, we reserve the right to block access to social networking sites from within the network if considered appropriate. If you accidently connect to a social networking site outside of permitted periods, you must disconnect immediately. If you consider that you need to access such a site during break times for a business-related purpose, please contact your Manage to seek assistance.

6.5 Employees and participants shall not engage, even in their own time, in any blogging or social networking that involves bullying, extremism views, anti - Britishness or harassment of, or making disparaging or derogatory comments about any employees or other participants or customers.

7. Internet

7.1 Education and Skills will ensure that the use of Internet derived materials by employees and participants complies with copyright law.

7.2 Participants will be taught how to be critically aware of materials they may see or are shown and how to evaluate and validate information before accepting its accuracy.

7.3 ESTD ensures that all shared resources/ forums and platforms contain checks to ensure these is no access to illegal or harmful content. In the event of this happening, content will be removed and an investigation into the content will take place. Appropriate action may be taken in accordance with the company policies and procedures. According to the online safety act, criminal offences cover:

* Threatening communications
* Trolling
* Intimate image abuse
* Cyber flashing
* Encouragement of/ assisting self-harm
* False information with the intent to cause harm

8. Monitoring

8.1 Education and Skills reserves the right to routinely monitor all users for the purpose of ensuring that the organisation’s rules are being complied with, investigating wrongful acts, or complying with any legal obligation.

8.2 Any breach of this policy is likely to result in sanctions being applied or disciplinary action being taken. A serious breach of this policy may be considered to amount to gross misconduct or dismissal. The following are non - exhaustive examples of the type of behaviour which may be regarded as gross misconduct:

• Posting confidential company, client or supplier information online;

• Any form of harassment, bullying, extremism grooming, radicalisation or discrimination against any of our employees, participants, workers, suppliers, clients or customers;

• Making derogatory, damaging or offensive comments or statements about any of our employees, participants, workers, suppliers, clients or customers;

• Online posting of personal data or information which you have obtained from Education and Skills about another employee or worker, without their consent;

• Any activity that may bring Education and Skills into disrepute or damage or lower the company’s reputation.

8.3 All employees and participants are encouraged to be vigilant and aware of potential illegal activity or misuse. The Safeguarding officer should be contacted immediately if any such activities may appear to be involved, including:

• Child sex abuse images;

• Adult material that potentially breaches the Obscene Publications Act;

• Criminally racist material;

• Other criminal conduct, activity or materials.

8.4 Complaints of internet misuse by participants will be dealt with by the Safeguarding Officer and recorded as a Safeguarding issue;

8.5 All complaints about employee’s misuse must be referred to the Safeguarding Officer who will liaise with the Quality Manager to investigate fully.

9. Equality Impact Assessment

9.1 This policy has been assessed for its impact on equal opportunities and has been informed by the aim to eliminate all forms of discrimination in all strands of the equal opportunities legislation.

10. Additional information

This policy should be read in conjunction with:

* Safeguarding Policy
* Whistle Blowing Policy
* Bullying and Harassment Policy
* Safer Recruitment Policy
* Prevent Policy
* Modern slavery Policy
* Prevent reporting procedure

Link to the government website on the Online Safety Act:

<https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer#what-the-online-safety-act-does>