Safeguarding Policy – Online Safety

Employment, Business and Skills

Document Owner: Celia Willson

Head of Programmes and Performance.

Reviewed: 9/6/2022

SUPPORTED BY MAYOR OF LONDON

Education & Skills Funding Agency

European Union European Social Fund

Waltham Forest

Safeguarding Policy – Online Safety

Our Vision: To create and target opportunities that connect our residents and learners with high-quality jobs, qualifications and supports our businesses, to raise the level of skills for life, work and wellbeing.

1. Introduction

1.1 Employment, Business and Skills has a duty of care to safeguard all learners / clients, staff, visitors, and stakeholders. It is committed to providing a totally safe and secure learning and training environment for both learning and work. This online safety policy should be read in conjunction with other relevant Service policies and Procedures such as Safeguarding and Prevention of Radicalisation Policy, IT User Policy, Learner Behaviour Policy and the Equality and Diversity Policy.

Employment, Business and Skills recognises the benefits and opportunities, which new technologies offer to teaching and learning. Our approach is to implement safeguards within the Service, and to support staff and learners / clients to identify and manage risks. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies.

Employment, Business and Skills (EBS) has expanded blended delivery approach in light of the current coronavirus pandemic. The service has updated online safety policy and procedure to ensure the safety of learners / clients on our online provision or in our venues. We will ensure that key Safeguarding principles are adhered and monitored, ensuring that all 'online working practices' to include the increased 'on-line workings' brought about through COVID-19, are placed at the centre of service delivery and safeguarding.

1.2 The policy applies to all EBS Staff and Learners / clients who have access to the Service IT systems, both on our premises and through remote access. Any user of Service IT systems must adhere to e-Safety Rules, regulations, and the IT Use Policy. The e-Safety Policy applies to all use of the internet, and electronic communication devices such as outlook email, mobile phones, laptops, PCs, iPads, social networking sites, and any other systems that uses the internet for connectivity purposes or through the providing of information.

It is of paramount importance to the service that:

- Staff understand their responsibilities to safeguarding in both centre based, community and online delivery.
- The service ensures safeguards on Service IT-based systems are strong, reliable and reportable
- Staff, learners, clients and stakeholders are educated in e-safety and follow

safeguarding policy and processes.

- User behaviour is safe and appropriate.
- Storage and use of images and personal information on EBS Service IT based systems is secure and meets all legal requirements
- Learners / clients in receipt of online blended courses / services, work placements are Inducted and supported through their course or employability / project lead.
- The service ensures any incidents, which threaten e-safety, are managed appropriately
- To ensure that any malpractice is addressed, and person or persons are disciplined or educated appropriately.
- EBS IT services communicates with Safeguarding Team to mitigate and educate Staff and Learners
- The service applies the same professional standards regardless of culture, disability, gender, language, racial origin, religious belief and sexual orientation
- Staff and managers continually monitor and review practice to ensure guidance is followed

1.3 A wide range of technologies are now used in education and employability provisions. Safeguarding learners / clients against the risks involved in using such technologies, often referred to as online safety, is an important part of an overall safeguarding strategy.

Employment, Business and Skills recognises that safeguarding learners / clients and providing them with the skills to safeguard themselves when using this technology, is a key aspect of the Services offer.

The Service also recognises that banning, blocking and filtering approaches, though useful, cannot be regarded as sufficient protection for learners / clients and it does not relieve the Service of a duty of care with regard to safeguarding learners / clients and employees.

Through a combination of effective policies and practice, a robust and secure technological infrastructure and education and training for learners / clients and staff, the Service has developed an effective online safety strategy across all learning and employability provision.

2. Definition of E-Safety

2.1 The term e-safety is defined for the purposes of this policy as the process of limiting and mitigating the risks to all EBS learners / clients. This policy acknowledges learners / clients who have EHCPs (Educational, Health and Care Plan) or are Under 19, young people and vulnerable Adults when using the Internet, Digital and Mobile Devises, Technologies (IDMTs) through a combined approach. By

implementing policies and procedures and creating an infrastructure through education awareness and training, underpinned by standards and inspection.

2.2 E-safety risks can be summarised under the following headings.

- Exposure to age-inappropriate materials
- Exposure to chatrooms or sites linked to grooming
- Exposure to inaccurate or misleading information
- Exposure to socially unacceptable material, such as inciting violence or hate crime
- Exposure to extremism or radical views (radicalisation)
- Exposure to communication with organisations linked with County Lines
- Exposure to right-wing views or intolerance to other views
- Exposure to illegal material, such as images of child abuse
- Illegal Downloading of copyrighted materials e.g., music and films or book

2.3 This strategy will:

• Provide a safe environment for all learners / clients and employees
• Adhere to legal responsibilities
• Ensure that technologies are used responsibly in order to support innovative and effective learning and teaching / service delivery.
• Educate learners / clients to identify the risks technology can present, and help them develop the skills they need to safeguard themselves
• Assess the risks presented by technology and develop appropriate policies and guidance to mitigate against those risks
• Involve managers, staff and learners in developing acceptable use policies and establishing reporting procedures for unacceptable use
• Promote a culture of online safety within the Service

3.1 Online safety risks can be broadly mapped across four areas:

Contact:

- Which may be unwelcome or inappropriate, including grooming or sexual contact

Commerce:

- Illegal activity such as phishing or identity theft

Content:

- This could include inappropriate or illegal content, material that incites racial hatred, condones and encourages support for terrorism and forms of extremism leading to terrorism or criminally obscene content.

- It also includes the inappropriate public posting of material. This may apply to employees equally as to learners, and may include the inappropriate and potentially unsafe posting of personal data, or the posting of material that

brings the individual or the provider into disrepute or impacts upon their business

Conduct:

- A person's dress and appearance are matters of personal choice and self-expression and some individuals will wish to exercise their own cultural customs as appropriate for a formal / professional environment
- Includes activities carried out against the learner and also those carried out by the learner. This category includes anti-social or illegal behaviour, and the ranges of behaviours and activities that make up cyber bullying, learner / client involvement and consultation
- Technological tools will be used effectively to manage and monitor the use of ICT
- Provision, to filter content, and to track and manage the use of systems, software and internet access
- Monitoring Procedures
- Emerging online safety incidents will be reported to the designated person in line with the Service safeguarding policy. Termly incident reports will be presented to the Safeguarding lead as appropriate

4.1 Staff Roles and Responsibilities:

- The Head of Programmes and Performance (ICT Lead) and Safeguarding Lead, Head of Skills are responsible for maintaining this policy, and for monitoring best practice in ICT procedures and practices to manage any e-safety risks effectively.
- All EBS Managers (SMT) for implementing good e-safety practice and safeguards consistent with this policy in their area of responsibility.
- All members of Service staff for staying alert to and responding appropriately to any potential or actual e-safety issue.
  Recordings and images with learners / clients in view or can be identified can only be stored on our Learning hub (as part of class resource), within the course code / project, for the academic year / or project term. Other consented recordings will be securely stored on LBWF cloud drive. DO Not use for promotional activities unless a consent form has been signed. Completed consent form should be sent to ebs.marketing@walthamforest.gov.uk in sufficient time to be viewed and approved prior to use).

5. Outcomes

5.1 ICT Security

The Service networks are safe and secure, with relevant, appropriate, and up-to-date security measures and software in place. EBS uses 'Barracuda' system as our firewall E-Safety protection. Barracuda protects us from flags

up security threats "outside world threats", enabling black and whitelisting categories and provides a filtering system to our Internet traffic. All websites accessed from EBS venues are compared with the list of "harmful websites" and the access is either granted or denied depending on the result. A list is provided by Barracuda and regularly updates EBS of issues or concerns. In addition, EBS also runs reports to review and address any concerns.

5.2 Risk assessment and training

When making use of new technologies and online platforms, all staff must assess the potential risks that they and their learners /clients could be exposed to. All staff and learners / clients are provided with opportunities to complete training on how to use Zoom, Microsoft Teams and how to appropriately share the screen and communicate. This is also reinforced through the EBS Learner / client Induction.

6 Behaviour and Responsibilities

- Staff should select a manner of dress and appearance appropriate to their professional role and which may be necessarily different to that adopted in their personal life. Staff should ensure they are dressed decently, safely and appropriately for the tasks they undertake; this also applies to online or virtual teaching.
- Staff are required to take into account issues such as accessibility within the family home, the mental health and wellbeing of learners including screen time, the potential for inappropriate behaviour by learners or staff online.
- All teaching / delivery staff have the responsibility of educating learners / clients in their care about safe internet practice, including the reporting of any unsuitable material that finds its way through the Service's web safety filter.
- Through continuous and appropriate staff development, the Service will seek to ensure that staff have the skills, knowledge and understanding required to both assess and mitigate against risks, and help learners develop the skills necessary to operate safely in a digital environment
- Staff are required to talk through online safety during learner / client induction.
- Staff are required to make learners / clients aware that some online sessions maybe recorded. It is important that learners / clients are aware and opt into recording. Please ask learners / clients and let them know they can switch their camera off if they don't want to appear in the recording, why the session is being recoded, where it will be held and for how long. Staff should think about the background; photos, artwork, identifying features, mirrors – ideally the backing should be blurred.
- It is an unacceptable to download or transmit any material which might reasonably be considered obscene, abusive, sexist, racist, defamatory, related to radicalisation, violent extremism or terrorism or which is intended to anger, update or annoy, harass or intimidate another person. This also applies to use of social media systems accessed from EBS IT Service

systems.

- All users of information technology will adhere to the standards of behaviour set out in the IT User Policy.
- All users of IT adhere to EBS Service guidelines when using outlook email, mobile phones, iPads, Laptops, social networking sites, games consoles, chat rooms, video conferencing and web cameras, Microsoft Teams, Zoom, Skype etc.
- Any inappropriate use or abuse of IT systems will be reported to the Head of Programmes and Performance and Safeguarding Lead. Any issues of bullying or harassment (cyber bullying) will be dealt with seriously, in line with staff and Learner / client behaviour and disciplinary procedures.
- Any conduct considered illegal will be reported to the police.
- Staff must take responsibility for moderating content that is posted online as part of their session.
- Staff should be aware of cyber bullying, grooming law and child protection issues and forward any concerns to a Safeguarding Lead. See posters at centres and on the Learning Hub.
- Staff must keep their personal and professional lives separate online.
- Staff must not have learners as 'friends' on social media sites that share personal information. (Facebook, WhatsApp, Personal Email, Personal Phone Number)
- Staff must not divulge their personal details online, staff are also advised to investigate and acknowledge privacy settings on sites to control what information is publicly accessible.
- Staff should maintain professional ethics and code of conduct in line with safeguarding.
- Staff are expected to adhere to the Service's equality, diversity and inclusivity policy always and not post derogatory, offensive or prejudiced comments online. This applies to internal and external staff communications.
- Staff will not harass, intimidate, bully or abuse work colleagues/learners online. Staff should think about what is being written and the tone and impact poor communications could cause. (if in doubt, check with a Manager)
- Staff entering a debate with a learner / client online should ensure that their comments reflect a professional approach. Progression Targets given should be constructive, communication etiquette must professional. (once an email has been sent it cannot be retrieved)
- Staff should not use their Service Outlook e-mail address to join sites for any personal reason or make their Service e-mail address their primary contact method.
- Staff need to be aware that any reports of them undertaking inappropriate online activity through their EBS profile and links them to the Service will be investigated through HR and could result in disciplinary action taking place.

6.2 Use of images and video

- The use of images or photographs is always encouraged in teaching and learning. Consent must be taken, and staff must ensure there is no breach of any copyright or other rights of another person.
- Staff and learners must be trained regarding the risks in downloading, posting or sharing images, and particularly in the risks involved in posting personal images onto social networking sites, In all cases consent to share images must be received.
- EBS staff must provide information to all learners / clients on the appropriate use of images, and on how to keep their personal information safe.
- Managers of Vulnerable Learners (EHCP and LLDD) must give training to learners on how to safely use IT devises and how to keep themselves safe on-line.
- Advice, guidance and approval from the Head of Programmes and Performance or Safeguarding Lead, Head of Skills if there is any doubt about the publication or concern linked to posting or downloading materials.

6.3 Personal information

Processing of personal information is done in compliance with the GDPR and Data Protection Act 2018 the 8 principals of Data Protection must be adhered to.
The Eight Principles of Data Protection
1. Fair and lawful
2. Specific for its purpose
3. Be adequate and only for what is needed
4. Accurate and up to date
5. Not kept longer than needed
6. Consider people's rights
7. Kept safe and secure
8. Not be transferred outside the EEA

All information is kept safe and secure and is not passed on to anyone else without the express permission of the individual. (HR and MIS)
No personal information is posted to the Service website/intranets without the permission of a senior manager.
Staff must always store and maintain learners' / clients' personal information safe and secure. If in doubt, contact Head Programmes and Performance for support.
All storage of Staff and Learner / client information must comply with GDPR regulations.
When using any online platform, all personal information is password protected.
No personal information about any individual is taken offsite unless the member of staff has the permission of their manager or GDPR lead. All information must be stored centrally and used in conjunction with EBS procedures.
Every user of any IT facilities must log off on completion of any activity, or ensure the room is locked if unsupervised, when they are physically absent from a device.
Every user must lock their PC when not in use.

Staff who have a EBS mobile devices must keep the devise safe when not in use. All sensitive information must be encrypted, and password protected.
Any personal data no longer required, is securely deleted. Receive support from Head of Programmes or ICT.

7. e-Safety Reporting Procedure Concern about a Learner

1. Seek advice from Head of Programmes and Performance or Safeguarding Lead, Head of Skills
2. If this is a Child Protection / Safeguarding it may be referred to LBWF internal / external organisations (Police or Social Service or External Agencies)
3. If the concern is against the law the Police may be contacted
4. If it is dealt with internally an investigation will be carried out.
5. Depending on the concern disciplinary action may be taken
6. All Policies and Procedures will be followed
7. Appropriate paperwork will be completed
8. Learner placed on the EBS Safeguarding or Risk Register
9. Learner monitored and supported

7.2 Concern about a Staff Member

1. Report to Strategic Head of Skills
2. Strategic Head of Skills will liaise the Head of HR and Head of EBS Department
3. Investigation will be carried out
4. Depending on the concern disciplinary action may be taken
5. If the concern is against the law the Police may be contacted
6. All Policies and Procedures will be followed
7. Appropriate paperwork will be completed

Website for staff and learners:
https://www.peoplefirstinfo.org.uk/staying-safe/staying-safe-on-line/

Website for staff:
https://www.foundationonline.org.uk/course/index.php?categoryid=34

Equality Impact Assessment / Safeguarding Considerations

Employment, Business and Skills Service is committed to the promotion of equality, diversity and providing a supportive environment for all members of our community. Our commitment means that this policy has been reviewed to ensure that it does not discriminate (either intentionally or unintentionally) any of the protected characteristics of age, disability, gender (including gender identity), race, religion or sexual orientation and meets our obligations under the Equality Act 2010.

Name of Policy/Procedure	**Feedback, Compliments & Complaints Policy & Procedures**
1. In what ways could this function have a negative impact on any of the groups above? What actions have been taken to eliminate these?	There could be resource limitations in helping learners to follow all the requirements of this procedure. We would explore all the options available to us in order to support all users in their understanding and application of the procedure and make reasonable adjustments to the procedure if required, for instance, providing information in alternative formats, assisting complainants in raising a formal complaint or holding meetings in accessible locations
2. In what ways could this function have a positive impact on any of the groups above? How will this function be used to eliminate discrimination, advance equality of opportunity and foster good relations between different groups? Are there plans that will further advance equality?	This policy aims to be an open access and all inclusive process. The annual review of Safeguarding will look to identify updated legislation and controls in place at EBS
3. What evidence supports your judgement eg. Observations, Consultations, expert opinions, quantitative or qualitative surveys. If the evidence is in the form of additional documentation where is this stored?	Comprehensive and up to date Safeguarding Records
4. Has this function taken into account and cross-referenced where appropriate to Safeguarding policy and procedures? Give	GDPR regulations have been considered and actions comply with data protection requirements.

Details.	