WESTMINSTER
ADULT
EDUCATION
SERVICE

WESTMINSTER ADULT EDUCATION SERVICE

E-Safety Policy

Ref No: LE11

Version:2

Owner:	Head of Learner Development	**Approved by:**	Signature of behalf of Executive Board Arinola Edeh	**Date of approval:**	4.9.2023
Effective From Date:	4.9.2023	**Effective To Date:**	31.7.2024	**Next Review Date:**	July 2023

1. Purpose

WAES has a duty of care to safeguard all learners, staff, visitors, and stakeholders. It is committed to providing a totally safe and secure learning environment for both learning and work. WAES 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 to identify and manage risks. We believe this can be achieved through a combination of security measures, staff training, learner induction and guidance and implementation of our associated policies.

This e-safety policy should be read in conjunction with other relevant Service policies Procedures such as Safeguarding and Prevention of Radicalisation Policy, IT User Policy, Learner Behaviour Policy and the Equality and Diversity Policy.

WAES 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 following COVID-19, are placed at the heart of teaching, learning, and safeguarding.

2. Scope

The policy applies to all WAES Staff and Learners who have access to the Service IT systems, both on WAES premises and through remote access.

Any user of Service IT systems must adhere to e-Safety Rules and regulations, and the wider elements within the IT user Policy. The e-Safety Policy applies to all use of the internet, and electronic communication devices such as outlook email, Microsoft teams, mobile phones, laptops, PCs, iPads, games consoles, social networking sites, and any other systems that uses the internet for connectivity purposes or through the providing of information.

3. Objectives

The objectives of the policy are to:

- To ensure safeguards on Service IT-based systems are strong, reliable, and reportable.

- To ensure user behaviour is safe and appropriate.

- To ensure that the storage and use of images and personal information on WAES Service IT based systems is secure and meets all legal requirements.

- To ensure that learners on Distance Learning and Apprenticeship courses are Inducted and supported through their Personal Tutor or Assessor and Employer.

- To ensure that WAES educate Staff and learners in e-safety, across there learner journey.

- To ensure 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.

- To ensure that WAES IT services communicates with Safeguarding to mitigate and educate both Staff and Learners.

4. Definition of E-Safety

The term e-safety is defined for the purposes of this policy as the process of limiting and mitigating all e-safety risks to all WAES learners.

This policy acknowledges learners who have Educational Health Care Plans (EHCPs) or are Under 19 or young people and vulnerable Adults when using the Internet, Digital and Mobile Devises and Technologies, through a combined approach.

By implementing policies and procedures and creating an infrastructure of education awareness and training, that is underpinned by standards and inspection.

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

5.1 Content

- 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 crimes.
- Exposure to extremism or radical views (radicalisation)
- Exposure to communication with organisations linked with County Lines.
- Exposure to right-wing views or being intolerant to other people's views.
- Exposure to illegal material, such as images of children, child abuse, sexual exploitation, or pornography.
- Illegal Downloading of copyrighted materials e.g., music, films, or books

5.2 Contact

- Grooming using communication technologies, potentially leading to sexual assault or child prostitution, sexual exploitation or inappropriate sharing of photographs or videos. It is important to note vulnerable adults are equally at-risk.
- Radicalisation the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups (Prevent Agenda)
- Extremist views and ideologies associated with Right Wing extremist views.
- Child Sexual Exploitation (CSE)

- Bullying via websites, mobile phones, tablets, or other forms of communication device
- Youth Produced Sexual Imagery (YPSI)–formerly known as 'Sexting')

5.3 Contact and Educate (the three Cs)

- **Content**: being exposed to illegal, inappropriate, or harmful material
- **Contact**: being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of causing harm

5.4 Commerce

- Exposure of minors (under 16) to inappropriate commercial advertising
- Exposure of Vulnerable Adults to commercial advertising (EHCP or Disability and Inclusion learners)
- Exposure to online gambling sites
- Exposure to on-line chat rooms sites
- Exposure to commercial and financial scams

5.5 Conduct

- Personal online behaviours that increase the likelihood and risk or has the potential to causes harm to individuals.
- Conscious online behaviour that entices and indoctrinates another person or persons to commit a crime.
- Conduct both internally at any WAES centers and on-line using a WAES device.

6 Responsibilities

- The Head of IT and Safeguarding Leads are responsible for maintaining this policy, and for monitoring best practice in IT procedures and practices to manage any e-safety risks effectively.

The following persons are responsible for implementing it at WAES:

- The Head of Human Resources for all e-safety matters in relation to WAES Staff.

- Safeguarding Leads for all e-safety matters in relation to support for Learners.

- The Head of IT will champion good e-safety practice in Service IT facilities and processes, and for providing any technical expertise when issues are under investigation.

- Head of IT is responsible for delivering and maintaining effective filtering and monitoring systems, providing a safe environment for learners and staff to learn and work and both online and offline.

- Head of Learner Development to ensure e-safety is incorporated into the WAES Learner Induction, supporting tutors with e-safety, and for providing an appropriate range of resources to tutors to access.

- Safeguarding Leads for delivering e-Safety training to all WAES staff and volunteers.

- Personal tutors for good e-safety practice as part of teaching and learning. For Distance Learning, provision tutors will take the responsibility for managing 'safe systems' whilst studying on-line. learners

- Issues raised by any apprenticeship learner or employer will be resolved through this department in conjunction with safeguarding.

- All WAES Heads and Co-ordinators for ensuring that e-safety is embedded into curriculum teaching and learning schemes of work. grammes.

- All WAES Managers (SMT) for implementing good e-safety practice and safeguards consistent with this policy in their area of responsibility.
- The Service Safeguarding Committee will be overseeing and reviewing e-safety arrangements.

- All members of Service staff must stay alert to and respond appropriately to any potential or actual e-safety issue.

7 Outcomes

7.1 IT Security

The Service networks are safe and secure, with relevant, appropriate, and up-to-date security measures and software in place.

The Head of IT will manage the WAES firewall and have responsibility for understanding the implementation, all upgrades and overall management of the system effectively, across all WAES centers.

The Head of IT will ensure that the firewall is monitored and updated regularly.

WAES uses 'Smoothwall' system as our firewall E-Safety protection. Smoothwall protects us from "outside world threats", separates different segments of our internal network and provides a filtering system to our Internet traffic.

All websites accessed from inside the college 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 Smoothwall and regularly updates WAES of issues or concerns.
In addition, WAES uses Sophos, which is another layer of internal protection that will detect potential viruses. Also, it hunts down any threats detected as active and adversaries on potential issues or concerns.
The Head of IT will know how and when to escalate concerns when identified to Safeguarding Lead. In most cases the firewall will trigger any log-in related to Prevent, sexual exploitation, hate crimes or pornography.

All staff concerns will be reported directly to Designated Safeguarding Lead.

7.2 Risk assessment and training

When making use of new technologies and online platforms, Quality, the Head of IT and Tutors must assess the potential risks that they and their learners could be exposed to.

Any on-line or hybrid teaching, staff and learners received training on how to use Microsoft Teams and how to appropriately share the screen and communicate, during lesson delivery. This is also reinforced through the WAES Learner Induction, available to all learners including, Distance Learning, Apprenticeship, Community Learners, and learners on short courses.

7.3 Behaviour and Responsibilities

- It is 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, or annoy, harass, or intimidate another person. This also applies to the use of social media systems accessed from WAES IT Service systems.

- All users of IT will adhere to the standards of behaviour set out in the staff IT User Policy. This is reinforced to learners during induction.

- All users of IT adhere to WAES 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 IT and Executive Board. Staff must not use a work computer for personal use.

- Any issues of bullying or harassment, often referred to as cyber bullying will be dealt with in line with the staff and Learner behaviour and disciplinary procedures.

- Any conduct considered illegal will be reported directly to the police. If a learner has been identified under Prevent, WAES safeguarding will communicate with our WCC representative.

If the learner has met the threshold, they will be referred to a Channel panel.

- Staff must receive consent for recording on-line lessons or taking photographs, this would include both enrichment activities and teaching.

- Staff must take responsibility for moderating any content that is posted online.

- Staff should be aware of cyber bullying and the impact this could have over learners and the sexual Offences act 2003, covering the grooming law and child protection issues. Staff requiring any advice or guidance should contact a Safeguarding Lead.

- 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 recognise that they are legally liable for anything they post online. Staff should maintain professional ethics and conduct in line with safeguarding.

- Staff are expected to adhere to the Service’s equality, diversity, and inclusivity policy and never post derogatory, offensive, or prejudiced comments online. This applies to all internal and external staff communications.

- Staff should not harass, intimidate, bully or abuse work colleagues or learners online. Staff should think about what is being written and the tone and impact poor communications could have. (If in doubt, check with a manager)

- Staff entering a debate with a student online should ensure that their comments reflect a professional approach. Any targets given should be constructive, communication etiquette must be professional. (Remember that once an email has been sent it cannot be retrieved)

- Staff should not post any comments online that may bring the Service into serious disrepute or that may damage the Service’s reputation with partner organisations, Parents, Carers, Guardians, Learners, or prospective learners. Strong customer service values must be adhered to.

- Staff who wish to debate or pass comments on professional issues through personal on-line sites must be aware that this may not reflect the Service’s views, even with a disclaimer, and must consider any postings extremely carefully.

- 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 WAES profile and links them to the Service will be investigated through HR and could result in disciplinary action taking place.

7.4 Use of images and video

- The use of images or photographs is always encouraged in teaching and learning. Consent must be taken, if it involves learners, 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.

- WAES staff must provide information to all learners on the appropriate use of images, and on how to keep their personal information safe.

- Managers of Vulnerable Learners (EHCP and Diversity and Inclusion) must give training to learners on how to safely use IT devices and how to keep themselves safe on-line.

- Advice, guidance and approval from the Head of IT or IT Support Officers if there is any doubt or concern linked to posting or downloading materials.

7.5 Personal information

- The processing of personal information must be done in compliance with the GDPR and Data Protection Act 2018. We must always adhere to the 8 principals of Data Protection

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 European Economic Area (EEA)

- All information must be 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. Information posted on Yammer must remain professional and comply with WAES staff code of conduct.

- Staff must always store and maintain learners' personal information safe and secure. If in doubt, contact the Head of MIS and Exams for support.

- All storage of Staff and Learner information must comply with GDPR regulations.

- When using any online platform, all personal information is password protected. Never share your password with anyone.

- 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 WAES 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 WAES 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 IT or Head or MIS and Exams if needed.

7.6 Education and Training

- Staff and learners are supported through training and education to develop the skills to be able to identify any on-line risks independently and manage them effectively.

- Staff should never open an email if dubious about the sender. If advice is needed contact IT

- The WAES Learner inductions contains a combination of e-safety support. This can be found in the sections WAES to be Safe and WAES to be Digital, within the on-line learner induction on SharePoint.

- Learners are guided and supported in e-safety across the curriculum and opportunities are taken to reinforce e-safety messages throughout teaching and learning.

- Learners know what to do and who to talk to where they have concerns about inappropriate content.

- Learners understand the support available to them when searching the internet, or where inappropriate websites are discovered as part of a random search.

- In lessons, learners are encouraged to question the validity and reliability of materials researched, viewed, or downloaded. They are encouraged to respect the copyright of other parties and to cite the references properly.

- All new WAES staff or temporary users receive training on the use of IT and Safeguarding and e- Safety. Staff are also asked to read the IT User Policy.

7. Incidents and response

- A clear and effective IT incident reporting procedure is maintained and communicated to learners and staff. Any updates are circulated to all staff in the form of a bulletin or part of the weekly / bi-weekly learner or staff e- news.

- Reports of any e-safety incidents are acted upon immediately to prevent, as far as reasonably practicably possible, any harm or further harm occurring.

- Action following the report of an e-safety incident by a learner could include disciplinary action, direct reports to external agencies, parents, or carer updates for EHCP learners or Vulnerable Adults (e.g., the Police or Channel Panel). An incident could trigger a review of internal procedures and safeguarding protocols with increased staff support for the affected learners. This could be a personal tutor or a safeguarding lead.

8. Associated Documentation/Linked Policies/Procedures

- Racial & Religious Hatred Act 2006
- Sexual Offences Act 2003
- Police & Justice Act 2006
- Computer Misuse Act 1990 (s1-3)
- Communications Act 2003 (s127)
- Data Protection Act 2018 (GDPR)
- Malicious Communications Act 2003 (s1)
- Copyright, Design & Patents Act 1988
- Public Order Act 1986 (s17-29)
- Protection of Children Act 1978 (s1)
- Obscene Publications Act 1959 & 1964
- Protection from Harassment Act 1997
- Regulatory of Investigatory Powers Act 2000
- Child Protection Act 2003
- Prevent Duty Guidance: for Further Education institutes in England and Wales 2015

9. Access to the Policy

- The policy will be published on the WAES Websites, WAES SharePoint under ‘Safeguarding’, and ‘Quality & Curriculum Hub – Policies”.

- This policy will be published on the WAES Induction under WAES to be Safe (safeguarding)

10. Monitoring and Review

This policy is owned by the Safeguarding Committee, all updates will be reflected in the staff training module e-Safety.

This policy will be reviewed annually, in conjunction with any KCSIE updates. This policy sits alongside the WAES Safeguarding and Prevention of Radicalisation Policy and Prevent Risk Register.

This Policy was given full approval through the Executive Board, Safeguarding Committee, Head of IT and SMT

The policy may also be reviewed where concerns are raised by the Designated Safeguarding Lead, or where an e safety incident has been recorded and has triggered new concerns.

Appendix 1

Key Terminology

Child Sexual Exploitation (CSE) may involve utilising the Internet and social media to identify potential victims or as a tool to coerce and blackmail children into performing sexual acts, both on and offline.

Youth Produced Sexual Imagery (YPSI –formerly known as 'Sexting') can be defined as 'an increasingly common activity among children and young people, where they share inappropriate or explicit images online'. This can include sharing indecent images of themselves or others via mobile phones, webcams, social media, and instant messaging.

Cyber Bullying. All staff should be aware safeguarding issues can manifest themselves via peer-on-peer abuse. This is most likely to include, but not limited to: bullying (including cyberbullying), gender-based violence/sexual assaults and Youth Produced Sexual Imagery (YPSI. Staff should be clear as to the school or college's policy and procedures with regards to peer-on-peer abuse."

GDPR -The General Data Protection Regulation is a European Union regulation on Information privacy in the European Union and the European Economic Area. The GDPR is an important component of EU privacy law and human rights law, in particular Article 8 of the Charter of Fundamental Rights of the European Union.

Appendix 2

Key Factors and information for Education Settings (DfE) important for Under 19 learners and learners classed as vulnerable (WAES Diversity and Inclusion and EHCP Learners, learners under 18)

Section35. All school and college staff should be aware that abuse, neglect, and safeguarding issues are rarely standalone events that can be covered by one definition or label. In most cases, multiple issues will overlap with one another.

Section36. Abuse: form of maltreatment of a child. Somebody may abuse or neglect a child by inflicting harm or by failing to act to prevent harm. Children may be abused in a family or in an institutional or community setting by those known to them or, more rarely, by others (e.g., via the internet). They may be abused by an adult or adults or by another child or children (peer on peer abuse).

Section 38. Emotional abuse: the persistent emotional maltreatment of a child such as causing severe and adverse effects on the child's emotional development. It may involve seeing or hearing the ill-treatment of another. It may involve serious bullying (including cyberbullying)

<u>Appendix 3</u>

e-Safety Reporting Procedure

Concern about a Learner

1. Seek advice from a Safeguarding Lead
2. If this is a Child Protection issue, the Safeguarding Lead will seek clarity from Designated Safeguarding Lead (DSL) the safeguarding lead may refer to external organisations (Police or Social Service or External Agencies)
3. If the concern is against the law the Police may be contacted
4. If the concern is dealt with internally an investigation must be carried out.
5. Depending on the concern disciplinary action may be taken.
6. All Policies and Procedures must be followed.
7. Appropriate paperwork will be completed.
8. Learner placed on the Safeguarding or Risk Register.
9. Learner monitored and supported.

Concern about a Staff Member

1. Report to Head of HR or Principal.
2. Head of HR will liaise with the Executive Board and Head of 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 must be followed.
7. Appropriate paperwork will be completed.

Equality Impact Assessment / Safeguarding Considerations

Westminster Adult Education 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	**E-Safety Policy**
1 If **Equality Impact Analysis** is not relevant to this function, give reasons. and proceed to section 5.	
2 In what ways could this function have a negative impact on any of the groups above? What actions have been taken to eliminate these?	This could only have a negative impact if we fail to acknowledge personal vulnerability, disability, or the overall wellbeing of a learner.
3 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 for the future that will further advance equality?	The general principle included in section 5-7 of this policy is designed to ensure that the well-being of all learners is fully considered in any e-safety concern and support for the learner given. The safeguarding and prevention of radicalisation policy sits alongside this policy and is designed to protect vulnerable groups.
4 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?	Consultation with staff at all levels, due regard for Prevent and the overarching safeguarding legislation. This policy will be stored centrally on SharePoint visible to all staff and learners. Staff training will he hosted that sits alongside this policy.

5 Has this function taken into account and cross-referenced where appropriate to **Safeguarding** policy and procedures? Give Details.	Secure storage of learner evidence, and permissions for photographs /video recordings to be sought as required under GDPR.

POLICY OWNER **Signed** **Date**	Annette Robson Head of Learner Development Greg Zalesny Head of IT updated 1.9.2023

Version Control Information

Version	Date	Revision Author	Summary of Changes
1	1.11.2021	A E Robson	New Format
2	I.9.2023	A E Robson	Full review following KCSIE updates