



Westminster Adult Education Service

E-Safety Policy

Ref No: LE11

Version: 4

Owner:	Head of Learner Development	Approved by:	Executive Board	Date of approval:	7.10.2025
Effective From Date:	1.9.2025	Effective To Date:	1.8.2026	Next Review Date:	1.7.2026



WAES VALUES – Indicate & comment on which values are attributed to this policy procedure

Value	✓	Comment
R espect – We are inclusive and fair and strive for equality in everything we can do.	✓	The Service aims to adopt the highest possible standards and take all reasonable steps in relation to the safety and welfare of children, young people and vulnerable adults. WAES uses a respectful whole College approach to safeguarding young people and vulnerable adults.
A spiration – We aim high for our learners and do not accept mediocrity.	✓	Removing barriers and supporting learners to improve confidence and aspirations
I nnovation – We strive for continuous improvement, embrace change and take risks, across all parts of the service.	✓	We embrace change and continuous improvements for our learners.
S ustainability – We always assess our impact on the environment, whether that be physical, social or economic.	✓	We are focusing particularly on the social and emotional and economic wellbeing of learners.
E xcellence – In all that our staff do, they strive to be the best they can be.	✓	Training for staff and education for learners



Westminster Adult Education Service Safeguarding and Prevention of Radicalisation Policy

This Policy covers the e-safety Elements of Safeguarding Children, Young People and Vulnerable Adults. This policy also recognises the importance of on-line safeguards regarding the Prevention of Radicalisation, exploitation and terrorism.

In-order for us to safeguard affectively and within the remits of the legislation attached to Safeguarding, safeguarding must communication with Staff, Parents, Carers, Social services, Adult Services, Local Authorities, Multi-Agencies and the Police as required.

This policy recognises the key updates from Keeping Children Safe in Education (KCSIE) and the National Concerns linked with all areas of Prevent to include Radicalisation, Terrorism (including self-initiated) Criminal Exploitation, Generative AI to include misinformation, disinformation and Fake News and Bullying.

This policy sets out to support Staff, learners, parents, employers and carers email safeguarding@waes.ac.uk as a safe and affective mechanism for communication.

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 teaching and learning but also recognizes the importance of staying safe and the safeguards that are needed within this area.

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, Safeguarding and Welfare support 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', are placed at the heart of teaching, learning, and safeguarding.

2. Scope

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

Any user of Service based IT systems must adhere to e-Safety Rules and regulations, this 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.

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 vulnerable learners who may also have Educational Health Care Plans (EHCPs) or are Under 19 are our priority group. Learners who have welfare needs such as mental health concerns are also classified as vulnerable under this policy and need monitoring.

By implementing policies and procedures, we are creating an infrastructure of education, awareness and training that underpins our safeguarding priorities.

3. Objectives

The objectives of the policy are to:

Acknowledge that IT has a lot of safeguarding risks, far more now than ever before, we must use a consistent approach and acknowledge that learners classified as vulnerable are more 'at-risk' of on-line harms. Educate learners about copyright, plagiarism, and digital rights. Promoting responsible use of digital resources.

Deliver training to staff, ensure that all new staff have a full induction into e-safety and all the elements that surround this area.

Support and educate learners with mitigating risks aligned to staying safe on-line, when support needs have been identified.

4. Risks and Mitigation

4.1 e-safety risks can be placed under the following headings

Learner Induction

- Learners will understand the key reasons for online safety and security and the personal controls they need to take, during the 'Learner Induction' stage. This includes Plagiarism and improper use of AI.

To Protecting Personal Information

- Preventing identity theft, fraud, and misuse of personal data.
- Encouraging safe sharing practices and strong password habits.
- Ensuring safeguards on Service IT-based systems are strong, reliable, and reportable.
- Ensuring that the storage and use of images and personal information on WAES Service IT based systems is secure and meets all legal requirements.

To Safeguarding Against Cyberbullying

- Promoting respectful online behaviours.
- Providing tools and support to report and manage bullying incidents.

Preventing Exposure to Inappropriate Content

- Using filters to block harmful inappropriate material.
- Educating users on how to recognize and avoid content, such as Radicalisation, exploitation, Hate material or explicit materials etc.
- Consistent monitoring of the Fire Wall, when triggered safeguarding leads informed.

Avoiding Online Predators and Scams

- Educating staff and learners to recognise suspicious behaviour and phishing attempts.
- Educate staff and learners about the dangers and risks of on-line

Promoting Digital Wellbeing

- Encouraging balanced screen time and healthy online habits.
- Raising awareness of the impact of social media on mental health.

Ensuring Safe Use of social media and Apps and legal use

- Understanding privacy settings and terms of service.
- Encouraging critical thinking about what is shared and with whom.
- Understanding copyright, plagiarism, and digital rights.
- Promoting responsible use of digital resources.

Supporting Responsible Online Communication

- Teaching netiquette (internet etiquette).
- Encouraging respectful and inclusive digital interactions.
- To ensure user behaviour is safe and appropriate.
- 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.

Generative AI:

- Monitoring self-assessment tool and cybersecurity standards.
- Addressing AI Risks, promote digital literacy and safe on-line behaviours, across all levels and abilities.
- AI is **controlled** through our filtering and monitoring system
- **Misinformation:** monitoring and talking out misinformation, disinformation (including "fake news"), and conspiracy theories.
- **Parent or Carer Education:** implementing training for Parents or Carers from most vulnerable groups. (Inclusive Pathways)

Filtering and Monitoring (Fire Wall) Expectations

- Conduct **annual reviews** of their filtering and monitoring systems.
- Have Fire wall (Filtering and Monitoring) as a standard agenda item at Safeguarding Meetings.
- Ensure **governors** are aware of the digital safety measures

4.2 Online Safety Awareness and Behaviours

WAES acknowledges the “**Four Cs**” of online risk **Content, Contact, Conduct, and Commerce**

	Definition	Risks Involved
Content:	Being exposed to illegal, inappropriate or harmful material	<p>Risks: Exposure to inappropriate or harmful material (such as pornography, violence, hate speech).</p> <ul style="list-style-type: none"> ○ Misinformation or disinformation (e.g., fake news, conspiracy theories). ○ Content promoting self-harm, eating disorders ○ Extremist ideologies.

<p>Contact:</p>	<p>Being subjected to harmful online interaction with other users</p>	<p>Risks: Grooming or exploitation by adults.</p> <ul style="list-style-type: none"> ○ Cyberbullying or harassment from peers. ○ Persuasive tactics used by scammers or predators. ○ Being drawn into exploitation for ‘others’ gain ○ Unwanted or inappropriate messages, including from bots or strangers
<p>Conduct:</p>	<p>Personal online behaviours that increase the likelihood of causing harm</p>	<p>Risks: Misinformation, Disinformation. Conspiracy theories now formally recognised as online harms.</p> <ul style="list-style-type: none"> ○ Sharing personal information or images inappropriately. ○ Engaging in risky challenges, dares or harmful behaviour on-line ○ Posting offensive or harmful content. ○ Cyberbullying
<p>Commerce</p>	<p>Financial risks and exploitation,</p>	<p>Risks: In-app purchases or scams targeting Children or Vulnerable Adults</p> <ul style="list-style-type: none"> ○ Exposure to gambling or loot boxes. ○ Manipulative advertising or influencer marketing. ○ Online scams and phishing

5. Online Abuse and Bullying

We need to have a greater emphasis on the **interconnectedness of online and offline abuse:**

- We accept that Bullying may include but may not be limited to **face-to-face or on-line** bullying, prejudice-based bullying or discriminatory bullying.
- Bullying Includes **non-consensual sharing of indecent images**, and **misogynistic content**.
- Greater awareness of the **‘On-Line’ apps** that can when used inappropriately can be a cause for concern, such as Facebook and Snapchat (been linked with Cyberbullicide)
- Having a greater understanding of ‘Cyberbullicide’ due to it being defined as **‘suicide indirectly or directly influenced by experiences with on-line aggression’**. Parents and

young people are frequently unaware of the risks and potential criminal liability associated with cyberbullying

- Gaming sites that can disguise discussions and collaborations around Right-Wing Extremism.
- **We have Increased controls regarding** managing all **low-level concerns** in the classroom, through recording and monitoring processes.
- Staff training and briefing covers the importance of on-line behaviours and the risks our vulnerable learners may have. The training also details the most common apps, linked with exploitation.

5.1 Prevent:

We integrate Prevent into our teaching: Staff are aware of what they need to look out for, such changes in behaviour or strong views within this area.

- We acknowledge the primary threat to London is from **Self-Initiated Terrorism (S-IT)**, rather than any specific terrorist group.
- S-IT actors can emerge from any ideology, acting without material support or direction from a terrorist group or organisation.
- S-IT attacks continue to pose the greatest threat within Extreme Right-Wing Threat. Ideologies are often mixed and fragmented, including racist, anti-LGBTQ+, misogynistic, anti-immigration and anti-establishment sentiments (amongst others).
- We acknowledge a significant amount of Extreme Right-Wing activity may not meet the terrorism threshold, with content rarely directing for attacks. **We do know a high volume of this activity takes place online.**
- Home Office legislation followed, staff are aware of what they need to look out for.
- **Educate Against Hate**, signposted directly from the Government Website.

5.3 Mental Health

Changes in learner behaviour: This could indicate a mental health concern (that may not have been disclosed to Welfare), behaviour changes in some cases can indicate that a person is suffering, or at 'risk of suffering'.

- Increased monitoring of all learners who have disclosed a 'Mental Health' problem, alongside Welfare Officers.
- Identification of learners who are 'struggling with work'
- Learners who have stopped taking medication consistently
- Changes in learner behaviour
- Changes in communications with tutor or learners
- Changes in appearance

- Awareness of key 'incel' behaviors

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 people 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 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 appropriate UpToDate training for all staff.
- 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 Curriculum Managers 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, Head of Quality, the Head of IT and Tutors will 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.

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.
- Staff must adhere to the standards of behaviour set out in the staff IT User Policy.



- 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 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, safeguarding will communicate with our WCC representative. If the learner has met the prevent threshold, they will be referred to a Channel panel.
- Staff must get consent for recording on-line lessons or taking photographs, including enrichment and careers activities and teaching.
- Staff must take responsibility for moderating any content that is posted online.
- Staff are aware of the impact of cyber bullying and on-line controls.
- 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. This includes (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.
- 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 all 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 device 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 of 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.

8. 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.

9. 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

10. Access to the Policy

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

11. 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

WAES Safeguarding Headlines for KCSIE 2025-26

Key updates in the Keeping Children Safe in Education (KCSIE) 2025

1. Online Safety

- **Generative AI:** New guidance on using generative AI is included, and the document directs us to the DfE filtering and monitoring self-assessment tool and cybersecurity standards.
 - Addressing AI Risks, potential risks associated with Artificial Intelligence, we must promote digital literacy and safe on-line behaviours, across all levels and abilities.
- **Misinformation:** The list of potential online harms has been expanded to specifically name misinformation, disinformation (including "fake news"), and conspiracy theories.
- **Parent or Carer Education:** WAES will be implementing training for Parents or Carers from our most vulnerable groups. (Inclusive Pathways).

2. Stronger focus on Vulnerable Groups

- **Vulnerable Groups:** Increased emphasis on safeguarding our most Vulnerable Groups, to include SEND learners and learners with disabilities, EHCP Learners, learners struggling with Mental Health or who are LGBTQ+.

3. Attendance: Increased monitoring across all vulnerable groups, especially EHCP learners or SEND learners.

- a. We must monitor attendance for all learners. EHCP and vulnerable learners must be tracked and the parent, carer and employer contacted.

4. Bullying:

- a. **Increased emphasis** on managing all **low-level concerns** in the classroom. Bullying is most likely to include but may not be limited to face-to-face or on-line bullying, prejudice-based or discriminatory bullying.
 - b. Consistent adherence to the Learner Behaviour and Safeguarding Policy. **All low-level/informal concerns** must be placed onto **EBS** 'Support Tutor- under Staff Message'. Any formal concerns must be recorded onto **EBS** 'Support Tutor- under Staff Concern, as well as following the **formal** disciplinary stages 1-4 (Behaviour Policy, full guidance).
- 5. Maintaining Clear Boundaries**
- a. **Maintaining professional boundaries:** Always following staff code of conduct, this applies to all staff. In some cases, staff may need to reinforce this area with learners.
 - b. Any Visitor or Contractor must be accounted for and supervised while in WAES.
- 6. Mental Health**
- a. **Changes in learner behaviour:** This could indicate a mental health concern (this may not have been disclosed at enrolment), or in some cases can indicate that a person is suffering, or at risk of suffering.
 - i. Increased monitoring of all learners who have disclosed a 'Mental Health' problem, alongside Welfare Officers.
- 7. Child Criminal Exploitation (CCE) or Child Sexual Exploitation (CSE):**
- a. **Awareness** that we have vulnerable young adults, who could easily fall within this category.
 - i. Safeguarding leads need to be alerted if a learner makes a disclosure within this area.
- 8. Violence against Women and Girls:**
- a. A key priority under 'Domestic Violence', this has now been given an abbreviation of VAWG (Violence against Women and Girls).
 - i. Coercive Control alongside VAWG are key areas the Safeguarding Leads are managing and signposting learners to external agencies.
- 9. Working Together:**
- a. **If you need any advice** or support regarding a learner or if you need to chat about a learner as you are concerned, contact a Safeguarding Officer or a Welfare Officer.
- 10. Prevent:**
- a. **We must integrate this into our teaching:** Understand the stages of Prevent and what we need to be looking out for, changes in behaviour or strong views within this area.
 - i. Remember, learners may have an ideology or no ideology.
 - ii. Home Office has developed training as an introduction to the Prevent duty:
<http://www.elearning.prevent.homeoffice.gov.uk/>
- 11. Further Reading:**
- a. Read through the updated guidance for in-depth information regarding Safeguarding:
[Keeping children safe in education 2025: part one information for all school and college staff](#)



Safeguarding Team September 2025

Appendix 2

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 Inform



ation 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 3

e-Safety Reporting Procedure

Concern about a Learner

1. Seeking 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
<p>1 If Equality Impact Analysis is not relevant to this function, give reasons.</p> <p>and proceed to section 5.</p>	

<p>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?</p>	<p>This could only have a negative impact if we fail to acknowledge personal vulnerability, disability, or the overall wellbeing of a learner.</p>
<p>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?</p>	<p>The general principle included in section 5-7 of this policy is designed to ensure that the wellbeing of all learners is fully considered in any e-safety concern and support for the learner given.</p> <p>The safeguarding and prevention of radicalisation policy sits alongside this policy and is designed to protect vulnerable groups.</p>
<p>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?</p>	<p>Consultation with staff at all levels, due regard for Prevent and the overarching safeguarding legislation.</p> <p>This policy will be stored centrally on SharePoint visible to all staff and learners.</p> <p>Staff training will be hosted that sits alongside this policy.</p>
<p>5 Has this function taken into account and cross-referenced where appropriate to</p>	<p>Secure storage of learner evidence, and permissions for photographs /video recordings</p>

<p>Safeguarding policy and procedures? Give Details.</p>	<p>to be sought as required under GDPR.</p>
---	---

<p>POLICY OWNER Sign/Date</p>	<p>Annette Robson Head of Learner Development</p>
---	---

Version Control Information

Version	Date	Revision Author	Summary of Changes
1	1.11.2021	A E Robson	New Format
2	1.9.2023	A E Robson	Full review following KCSIE updates
3	3.9.2024	S Whitehouse	No Change – New Front Cover
4	1.9.2025	S Whitehouse	No Change – New Front Cover KCSIE Updates only