WEA E-Safety Policy

1. Purpose

The aim of this Policy is to set out the WEA's arrangements, advice and requirements for promoting the safety of WEA students, staff, members and other stakeholders when digital tools and resources on and offline.

2. Value

The WEA recognises the benefits and opportunities which digital information technologies offer to all aspects of the WEA's business, education and voluntary organisation. We provide a range of facilities, hardware, software, networks and communications infrastructure to staff, students, members, volunteers, partners and the public. In addition we promote the use of appropriate devices, particularly by students, but also by staff, members, volunteers, partners and the public to access and use WEA and other information, learning and other resources to support their engagement with the WEA. These devices may be owned and controlled by the WEA but usually they are not. Students in particular but also a wide range of other stakeholders will use their own devices or devices owned by a third party.

Digital information technologies are increasingly at the heart of educational practice supporting the acquisition of knowledge, skills, and understanding, promoting achievement and enabling lifelong learning. They are not merely useful tools they are increasingly central to the education process itself.

However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges arising from the use of these technologies.

This policy seeks to explain the principles of the WEA approach to e-safety and to highlight the likely practical steps implied by the policy. It does not provide detailed guidance on every eventuality in this complex and changing area. Rather practice should be based on these principles according to the specifics of each scenario that is faced.

3. Scope

The policy applies to all staff, students, members, volunteers, partners and other stakeholders of the WEA

The e-Safety Policy is concerned with

- The use of digital equipment, tools, systems and resources by WEA stakeholders and the public in pursuance of their roles and responsibilities that arise from their involvement in the WEA's purposes.
- The inappropriate use of these same systems arising as a result of a WEA stakeholder's access to these systems because of their legitimate connection with the WEA.

The Workers' Educational Association (WEA) is a charity registered in England and Wales (number 1112775) and in Scotland (number SC039239) and a company limited by guarantee registered in England and Wales (number 2806910)

- Ensuring that procedures are in place to manage Safeguarding and Prevent Duty concerns in relation to digital safety
- In relation to this policy, systems will include appropriate and inappropriate use of personal digital communications and social media when the use arises out of the stakeholder's connection with the WEA.

4. Principles and Approach for E-safety in the WEA.

The WEA is a provider of education to adults. Our teaching and learning primarily takes place in premises and venues not owned or controlled by the WEA. It usually takes place in in community settings and the use of particular venues may be short term. Many venues will not have dedicated computer facilities for educational use and WEA students will typically use their own digital equipment.

The WEA has therefore created an approach which responds to these particular challenges. The key features of this approach are as follows –

a) Support all WEA stakeholders but particularly students, members and volunteers to gain and maintain a strong awareness of the safety challenges and risks posed by the use of information technologies. These include
    - Protecting their devices with appropriate security protocols.
    - Protecting their personal information and identities with appropriate security measures and practices for the social information world so that they only share information that is sensible and desirable from their point of view.
    - Having a good awareness of key risks, such as Trojan horse emails, phishing and "too good to be true" offers and how to respond to them effectively.
    - Recognising cyber bullying, sexual and ideological grooming and threatening behaviours and responding to them appropriately.
    - Identifying and responding to viruses and malware etc.

b) Supporting WEA Partners who own or control premises used by WEA personnel and stakeholders to take reasonably practicable steps to enhance safety for users of their premises and services.

c) Where WEA stakeholders are using WEA owned and controlled equipment, software networks and communications infrastructure that all reasonably practicable measures are taken to ensure appropriate usage that is safe, responsible and professional.

d) Where it is within the WEA's control using appropriate measures and policies to protect the personal data of our stakeholders and where it is not within our control actively promoting sensible and sensitive information protection in compliance with any appropriate legislation.

In short our approach is to implement appropriate safeguards within the WEA which will support staff and students to manage any potential risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies.

5. Communications and Behaviour including social media and images.

Online communication and behaviour just as offline communications involving staff and WEA stakeholders including students must be courteous and respectful at all times. It should model the WEA's commitment to equality, diversity and respect at all times. Incidents of inappropriate behaviour, bullying or harassment, grooming or other unacceptable conduct will be treated seriously and in line with the student or staff codes of conduct and may result in disciplinary action up to and including gross misconduct or other appropriate sanctions. Where behaviour does not directly involve WEA related personnel we will report conduct to other organisations, if appropriate.

All digital communications involving staff, students, members and volunteers and other WEA stakeholders must be professional at all times. Staff and other WEA personnel in a position of trust should be appropriately sensitive to their role as a representative of the WEA and to their status as a privileged position in respect of the expectations of other WEA stakeholders. The use of social media is appropriate for communications when it is clearly part of the agreed means of interaction between groups of stakeholders. E.g. between a tutor and students in a class. Any connection with students, members or volunteers on social media in a personal capacity, whilst not necessarily inappropriate, must be mindful to maintain the professional relationship that a staff member may have with them.

It is always appropriate for any student or other similar stakeholders to withdraw from any social network or communication forum at their discretion for whatever reason.

Whilst in general this is usually the position for staff too, there are occasions where the WEA may require participation in some social networks in order to conduct WEA business.

Images or photographs of groups of people, online or in course work or marketing material should, in general, only be used where appropriate permission and consent has been given by the subject(s) of the photograph / image. Consent should also be sought for the use of any names or details of the subjects online or in course work. Exceptions to this rule should be considered and may include images of people already widely used and distributed such as those in the news etc.

The WEA will always take down images of people where it is made clear to the WEA that the image does not have the permission of the subject or that permission has been rescinded or for reasons of taste and decency when this is brought to the attention of the WEA.

6. Training and guidelines to support the policy

a. Staff

All tutors and education staff are trained in Safeguarding and Prevent procedures which include the risks and challenges involved in the safe use of digital resources. Training will be reinforced through the use of ZOOM video training and incorporated into sessions on the WEA approach to using digital resources to help students learn.

A link to the WEA e-Safety Guidelines will appear when users log on to the WEA intranet.

b) Students:

Issues associated with e-safety are likely to arise across the curriculum and students will receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies This will be provided at student induction and at appropriate points during the course. Students will be given information about what to do and who to talk to if they have concerns about inappropriate content . Within classes, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded.

E-safety guidelines are highlighted in posters and leaflets in classrooms.

7. **The Responsibilities of Staff:**

All staff are responsible for using IT systems and mobile devices on WEA business in accordance with the WEA ICT Use policy. Staff are responsible for attending staff training on e-safety and modelling equal, respectful and professional behaviours to students / other stakeholders at all times.

All staff must apply relevant WEA policies and understand the incident reporting procedures.

Education Core Staff must ensure that the tutors they manage are aware of this policy and that during the use of digital resources in their course programme tutors are aware of their responsibilities and have the necessary information resources to support students on e-safety matters.

Tutors are responsible for ensuring that students receive information on e-safety at the start of the course as part of student induction, and throughout courses where digital resources are used to promote learning. Students must be made aware of the code of conduct and appropriate behaviour in the use of electronic communications. All students must be aware of how to report a concern and to whom, in line with the Safeguarding procedures

Student Support staff and voluntary member staff must ensure that information and advice to students, members and volunteers includes e-safety support, information and training where appropriate.

Other WEA core staff will need to be aware of and apply the principles of this policy in their day to day work and interactions with WEA stakeholders.

8. Roles and Responsibilities of those concerned with implementing the policy

There are clear lines of responsibility for e-safety within the WEA.

The **WEA National Safeguarding and Prevent Lead** is responsible for managing and reviewing any e-safety incidents involving students, in association with the relevant Regional

Safeguarding Designate who is responsible for investigating any incidents or concerns and liaising with the local authority and external agencies, as appropriate.

The **Digital Curriculum and Quality lead** is responsible for leading a team of regional digital champions in the development of digital resources to help students / other stakeholders learn and in training staff / tutors / volunteers in the application of e-safety.

The **ICT Manager** is responsible for all aspects of Data Protection and the security of WEA computing and electronic data systems.

9. Reporting incidents or concerns

E-safety Incidents will be reported to the Regional Safeguarding Designate who in consultation with the WEA national Safeguarding and Prevent lead will oversee the investigation, including reporting to and taking advice from appropriate external agencies where necessary.

a) Incidents involving students:

All staff are responsible for ensuring the safety of students and should report any concerns immediately to their Regional Safeguarding Designate or line manager, using the Safeguarding reporting procedures.

All students should be aware of how to report a concern and to whom, in line with the Safeguarding procedures. In most cases this will either be their tutor or the Regional Safeguarding Designate. Students are provided with this information in the Student Handbook and on the Safeguarding poster discussed by the tutor during student induction.

b) Incidents involving staff:

The WEA is committed to ensuring staff safety. We expect staff to maintain appropriate professional boundaries in communications with students and in the use of social media. Safeguarding procedures will also apply to staff and volunteers should they receive inappropriate communications from students or other stakeholders.

Misuse of computers and other WEA ICT facilities including PCs, laptops, tablets, smartphones and email is a serious offence and will be dealt with appropriately through application of the WEA's Disciplinary procedure and, in some cases, reported to the police or the Disclosure and Barring Service. Employees will be held responsible for any actions that are taken against the WEA by a third party arising from restricted and/or offensive material being displayed or sent as a result of their actions whilst undertaking WEA business. Further information, including examples of misuse is provided in the ICT Use Policy.

If there is a concern about a member of staff or volunteer's behaviour in relation to ICT use, this should be reported initially to their line manager or the HR Business Partner and advice should be sought from the Regional or National Safeguarding Officer. Alternatively, the procedures outlined in the whistleblowing policy may be used.

c) Exemplar Concerns

Incident or concerns involving could include:

- Cyber-bullying via websites, social media, mobile phones or other technologies
- Cyber stalking
- Safeguarding issues such as on-line grooming, exploitation and/or radicalisation
- Sexting; the sending of sexual texts, images or videos.
- Viewing of inappropriate material, including accessing extremist websites
- Exposure to inappropriate advertising, online gambling or financial scams.
- Inappropriate use of social media, for example involving abuse, threats or rudeness to staff members or other students.

Please note: This is not an exhaustive list; there are many other reasons that concerns could be raised. All concerns should be appropriately considered and if necessary investigated.

When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved. The WEA Safeguarding or Prevent policy and procedures must be followed.

10. Security

WEA networks use industry standard approaches to keep information safe and secure. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of WEA systems and information.

WEA does not control many of the networks that WEA stakeholders use. WEA will provide advice on appropriate safety considerations such as refraining from using personal information or passwords over public wifi networks in education centres.

11. **Personal Information**

Any processing of personal information needs to be done in compliance with Data Protection legislation. This is likely to include content such as student records, e-portfolios and assessed work. The WEA is legally obliged to take steps to minimise the risk that data will be lost and processed unfairly.

12. Risk Assessment

Major WEA systems are assessed for e-safety as part of commissioning specification and ongoing maintenance.

13. Related Policies

This policy should be used in conjunction with other relevant policies, in particular:

Safeguarding policy and procedure

Prevent policy

Student Computer Use policy

Student Code of Conduct

Unacceptable student behaviour procedure

Staff Discipline policy

Data Protection policy

Staff Code of conduct

ICT Use policy (staff)

Whistleblowing policy

WEA code of conduct

Discipline policy

The policies can be accessed from:

https://intranet.wea.org.uk/hr/policies-and-procedures

The Workers' Educational Association (WEA) is a charity registered in England and Wales (number 1112775) and in Scotland (number SC039239) and a company limited by guarantee registered in England and Wales (number 2806910)