WEA Online Safety Policy in Teaching and Learning

1. Purpose

To set out the WEA's approach, arrangements and requirements for promoting the online safety of WEA learners, staff, members and other stakeholders in teaching and learning.

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.

2. Values

The WEA believes that learners have an entitlement to use digital technology for learning, working and living. The WEA will use online learning technologies wherever they enhance the learning experience for learners. The WEA recognises the transformational benefits and opportunities which digital information technologies offer to all aspects of the WEA's business, education and voluntary organisation.

A wide range of digital technologies are at the heart of educational practice supporting the acquisition of knowledge, skills, and understanding, enabling collaborative and peer-reviewed learning, promoting achievement and enabling lifelong learning. They are not merely useful tools; they are increasingly central to the education process itself.

Our expectations are that digital learning will build confidence, resilience, active engagement, participation and ownership of own learning.

WEA is aware of the potential risks and challenges arising from the use of digital technologies and seeks to avoid or mitigate these wherever it is reasonably practicable to do so.

3. Scope

This policy applies to all staff, learners, members, volunteers, partners and other stakeholders of the WEA engaged in teaching and learning activity. In most cases learners will be using their own devices to engage with WEA provision and learner support. In exceptional circumstances WEA provides some equipment on loan through the Discretionary Learner Support fund.

Other related policies (a full list can be found in Section 6):

- The Learner Computer and Digital Use policy applies to learners using WEA equipment as part of their learning journey.
- The WEA Acceptable Use Policy applies to WEA staff using WEA equipment and information services.
- The ICT Security Policy sets the WEA's approach to managing the threats and risks to WEA data assets by reducing them to an acceptable level.
- The WEA GDPR policy sets out the processing and security of personal data.

4. Approach

The WEA is a provider of education to adults. Our teaching and learning takes place:

- using Canvas, our virtual learning environment (VLE), to support the learning journey, enabling learners to communicate and work with their tutors and other learners, complete activities, assignments or homework, see feedback from tutors, and create opportunities for further research and reflection. Learners, tutors and staff all use Canvas
- with EBS, our Learner Record System in which learners have their Individual Learning Plan (ILP). All learners in England receive a WEA email address which is used to access EBS and Canvas
- face to face learning via our online classrooms using Zoom or Teams
- in venues operated by the WEA where digital equipment is a mixture of WEA and learner's equipment
- in community premises and venues not owned or controlled by the WEA. The use of particular venues may be short term. Many venues will not have dedicated computer facilities for educational use and WEA learners will typically use their own digital equipment.

The WEA's approach to online safety involves a combination of training, guidance, security measures and implementation of our policies to:

a) provide information and advice to all WEA stakeholders but particularly learners, tutors, and volunteers to gain and maintain an awareness of online safety challenges and risks and how to manage them

b) clarify roles and responsibilities, underpinned by training and support

c) identify online safeguarding behaviours or concerns and knowing how to report them.

a) Identifying and managing risks

The WEA provides information and advice to all WEA stakeholders on the safety challenges and risks posed using online technologies. Within the context of teaching and learning, learners, tutors, and volunteers this includes:

- protecting devices and personal details
- keeping safe and secure while learning with the WEA, including when learning with Zoom / Teams and Canvas
- recognising online safeguarding risks and knowing how to report concerns.

Use of messaging apps

To support safe, transparent and inclusive communication and learning environments, messages and emails are sent using WEA digital systems such as Canvas, Office 365 and EBS as appropriate. These use wea.ac.uk emails, meaning that personal details do not need to be shared, and IT and Digital teams can support these systems.

The WEA does not use or support the use of messaging apps (e.g. WhatsApp, Facebook, Telegram, Signal and others) for communications sent to, from or between learners, staff, members and volunteers.

Appropriate use of Canvas to communicate can support other teaching and learning activities in Canvas (e.g. gradebook, discussions, assignments). In Canvas, tutors can message learners and learners can message each other.

Tutors must only message or communicate with learners using Canvas. No other email or messaging app must be used by tutors to communicate with learners.

Whilst we cannot enforce whether learners use messaging apps with each other, we strongly encourage learners to use Canvas to communicate with each other, instead of using messaging apps.

Our approach includes providing information, advice and support to all WEA stakeholders to make safe and effective use of WEA digital systems and use of wider digital technologies.

b) Roles and responsibilities

All online behaviour involving staff, learners, volunteers and other WEA stakeholders must be professional, courteous and respectful.

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

All staff and volunteers must apply relevant WEA policies and understand the incident reporting procedures (see below).

The **WEA National Safeguarding and Complaints Managers** are responsible for managing and reviewing any online safety incidents involving learners, investigating any incidents or concerns and liaising with the local authority and external agencies, as appropriate. In addition, there are trained Safeguarding Designated Officers across the WEA.

The **Teaching and Learning Digital Development Manager** is responsible for leading a team of digital developers supporting tutors to help learners stay safe.

The **Tutor Training and Development Partner** is responsible for ensuring online safety is addressed through tutor and support worker training.

The **IT Director** is responsible for data and computer use policies and the security of WEA computing and electronic data systems.

The **Head of Policy, Risk and DPO** is responsible for GDPR policies and procedures and guidance and training.

c) Training, support and information

Staff

All tutors and education staff receive mandatory training in Safeguarding and Prevent procedures which includes the risks and challenges involved in the safe use of online resources, training on GDPR and online safety in Zoom/ Teams and Canvas training.

Tutors are responsible for ensuring that learners receive information on online safety at the start of the course as part of learner induction, and throughout courses where digital resources are used to promote learning.

Learners

Online safety is likely to arise across the curriculum and learners will receive guidance on online precautions and safeguards as appropriate. This will be provided through:

- Learning Agreement
- Learner Handbook which includes online safety - what to do and who to talk to if they have concerns about inappropriate content, communications or conduct as well as protecting their devices and personal data.
- online information in Canvas
- posters available for tutors to use with their learners.

Volunteers

Volunteers need to be aware of and implement this policy when they are in contact with and/or working with learners.

5. Safeguarding and reporting incidents or concerns

Procedures are in place to manage the Safeguarding and Prevent Duty concerns in relation to online safety.

Example safeguarding concerns

- Online bullying via websites, social media, mobile phones or other technologies
- Online sexual harassment
- Online stalking
- Online 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 learners.

Please note: this is not an exhaustive list; there are many other reasons that concerns could be raised.

Reporting online safety concerns

All concerns should be appropriately considered and if necessary investigated. When informed about an online 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 and Prevent policies must be followed.

Online safety incidents will be reported to the Safeguarding Designates who in consultation with the WEA national Safeguarding and Complaints Managers will oversee the investigation, including reporting to and taking advice from appropriate external agencies where necessary.

Incidents involving learners

All staff are responsible for ensuring the safety of learners and should report any concerns immediately to a Safeguarding Designate or line manager, using the Safeguarding reporting procedures. All learners 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 a Safeguarding Designate. Learners are provided with this information in the Learner Handbook, in the Safeguarding section of Canvas and discussed by the tutor during learner induction.

Incidents of inappropriate behaviour, bullying or harassment, grooming or other unacceptable conduct will be treated seriously in line with the Learning Agreement and may result in disciplinary action up to and including gross misconduct or other appropriate sanctions. We will also report conduct to other organisations, if appropriate.

Incidents involving staff

The WEA is committed to ensuring staff safety. We expect staff to maintain appropriate professional boundaries in all behaviour and communications. Safeguarding reporting procedures apply equally to staff, members and volunteers should they receive inappropriate communications or behaviour from learners or other stakeholders.

If a member of staff has a concern about the behaviour of another member of staff, Association member or volunteer in relation to the WEA Acceptable Use Policy, this should be reported initially to their line manager or HR and advice should be sought from the Safeguarding Designates or National Safeguarding and Complaints Managers. Association members or volunteers having a concern about the behaviour of a member of staff, or another Association member or volunteer in relation to the WEA Acceptable Use Policy should report their concerns initially to HR and advice should also be sought from the Safeguarding Designates or National Safeguarding and Complaints Managers.

6. Related Policies

This policy should be used in conjunction with other relevant policies.

The following policies can be accessed from: https://www.wea.org.uk/resources/policy-docs

Safeguarding Policy (includes Safeguarding Online Policy)

Prevent Policy

Sexual Harassment Policy

Learner Computer and Digital Use Policy

Unacceptable Learner Behaviour Procedure

Data Protection (Privacy) Policy

Whistleblowing Policy

The following policies are on the WEA Intranet or available on request:

WEA Code of Conduct

Discipline Policy

Bring Your Own Device Policy

WEA Acceptable Use Policy (WEA equipment and information services)

ICT Security Policy

Date of this Review	Date of next Review	Policy reviewed and updated by:	Policy approved by:
February 2024	July 2025	Teaching and Learning Digital Development Manager and Safeguarding and Complaints Managers	Director of Curriculum, Quality and Safeguarding