Adult Learning Within Reach

wea.org.uk

# Data Protection Policy

**Owner** **Information Governance Team**

**Approved by** **Head of Policy and Risk**

**Next review date:** **July 2026**

| Version Number | Date of Issue | Author | Status | Comments |
|---|---|---|---|---|
| 1 | May 2025 | Nancy Ho | Policy draft | Policy review |
| 2 | May 2025 | Policy Development Partner | Review | Policy review, format changes and standardisation of policy format. |

This policy and any related annexes will be reviewed by the Audit and Risk Committee. The policy will be reviewed every 12 months.

## 1. Introduction

Data protection laws give people legal rights regarding how their personal data is processed. These rights apply to you, as well as to every individual whose personal data you process while working with us.

Workers' Educational Association (WEA) (sometimes referred to throughout this policy as "we", "us" or "our") have obligations under these data protection laws regarding how we treat the personal data we hold, what we do with it and who we share it with. We take our obligations seriously and will take all appropriate steps to comply with these laws as we consider this critical to our business.

Data protection legislation is enforced in the UK by the Information Commissioner's Office (ICO), who can investigate complaints, audit our use of personal data and take action against us (and in some cases against you personally) for breach of this legislation. Enforcement action may include fines, criminal prosecution and preventing us from using personal data, which could prevent us from carrying out our business.

Breaches of data protection legislation could also lead to compensation claims from individuals who are affected.

The WEA is a Data Controller registered with the Information Commissioners' Office, with registration number Z4686639.

## 2. Purpose

The purpose of this policy is to:

- Outline how the WEA manages, protects and uses personal data to ensure compliance with legal and regulatory requirements.
- Establish a framework of data privacy, confidentiality and security to minimise the risk of unauthorised access and misuse of personal data.
- Define the roles and responsibilities of individuals within the organisation in relation to the handling of personal data.

## 3. Scope

This policy applies to:

The whole of the WEA, and to all its activities. It applies to all Personal Data and all other information that can reasonably be sensitive or confidential that is held or processed by the WEA. The WEA is a Charity registered in England and Wales (Charity number 1112775) and in Scotland (Charity number SC039239). The WEA is a company limited by guarantee which is registered in England and Wales, having registration number 2806910. In this policy references to "you" mean anyone that processes personal data on behalf of the WEA.

- The WEA in England; the WEA in Scotland; WEA Branches; members of professional staff, tutors, learners, volunteers, members; and service providers, partner organisations, contractors, consultants, affiliates, advisors and any other temporary staff engaged by the WEA.

## 4. Key responsibilities

The Information Governance Team is responsible for the maintenance, regular review and updating of this policy in collaboration with the Data Protection Officer (Head of Policy and Risk). All staff and volunteers should familiarise themselves with this policy and apply the contents of the policy to how they handle and process data. If anyone is unclear about any aspect of the policy, they should consult with the Information Governance Team for guidance.

## 5. Key terms used in this policy

**Personal data** is information (in any format) that relates to a living individual who can be identified from that information, either on its own or when it's combined with other information held by us. For example, names, addresses, contact details, salary details, job titles, Curriculum Vitae's (CV's), CCTV images, course recordings, participant recordings, credit card numbers, logon credentials, marketing preferences and data gathered from website cookies are all capable of being personal data.

**Processing** personal data means any activity carried out in relation to personal data, including collecting, recording, organising, storing, retrieving, altering, using, disclosing, archiving and destroying personal data.

**Data subject** is a term used to describe the individual to whom the personal data relates. For simplicity, in this policy, we sometimes refer to these people as 'individuals'.

**Special category personal data** (sometimes referred to as special personal data or sensitive personal data) is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, criminal convictions and offences, genetic or biometric data (where it's processed to uniquely identify someone), data concerning health or someone's sex life or sexual orientation.

## 6. Arrangements

### Data Protection Officer

The WEA employs a dedicated Data Protection Officer (DPO) as required by the General Data Protection Regulation (GDPR) as the organisation processes personal and special category data for a high volume of data subjects.

The WEA will ensure that the Data Protection Officer is independent, adequately resourced and reports to the highest management level via the Chief Operating Officer structure.

### Roles and responsibilities

- **The Data Protection Officer (DPO)** has responsibility for informing, advising, and monitoring compliance with the Data Protection Act and UK GDPR.
- **The Information Governance Team** is responsible for assisting the DPO in data protection activities to support compliance. This includes the development of data protection guidance and procedures, managing information requests, and managing data protection records.
- **The Senior Information Risk Owner (SIRO)** is responsible for the overall risk arising from the processing of personal data by the WEA.
- **Information Asset Owners and Administrators (IAO/IAA)** are responsible for ensuring data protection compliance in relation to their information assets. This includes the completion of Information Asset Registers and Records of Processing Activity.
- **All staff, including Core and sessional staff, volunteers and consultants**, should ensure that they adhere to the points set out in this policy when processing any personal data.
- **Line managers** are to ensure that those who they line manage, have read, understood and adhere to this policy.

### Lawful basis for processing personal data and special category personal data

The WEA will take all steps to ensure that all personal data collected as part of our business processes is assigned a **lawful basis.** The lawful bases which are most likely to be relevant to WEA processing are: consent, contract, legal obligation, vital interests, public task and legitimate interests. We also adhere to all relevant government legislation and directives when processing personal data.

The WEA will take all steps to ensure that any special category personal data collected as part of our business processes is assigned an additional **special category lawful basis** as defined in Article 9 of the General Data Protection Regulation (GDPR).

Adult Learning Within Reach



## Records of processing activities

The WEA holds a record of all its data processing activities within a Records of Processing Activities (ROPA) document. This record includes specific information about each activity including the purposes for processing, data sharing information, the lawful basis for processing and any joint controller details.

## Privacy Notices

To be fair and transparent about our processing activities, the WEA provides individuals with clear information about how we process their personal data. This information is referred to as a **privacy notice.**

Privacy notices are made available to data subjects at the point of data collection, whether this is via a website, a paper form or over the telephone. The WEA will take steps to ensure this information is concise, transparent, intelligible and in an easily accessible form, using clear and plain language.

All WEA Privacy Notices include:

- The controller's identity and contact details
- The Data Protection Officer's contact details
- What personal data is processed
- The purposes of the processing
- The lawful basis for the processing
- Who the personal data will be shared with
- Details of any international transfers of personal data
- The period for which data will be stored
- Details of any automated decision making using the personal data
- Details of the data subject's rights and how they can exercise these
- Details of how to complain to the Information Commissioner's Office if unsatisfied

## Storage limitation of personal data

The WEA will only keep personal data in a form which permits us to identify the individual concerned for as long as is necessary for the purpose(s) for which it has been collected. The WEA will ensure that personal data is not retained for longer than is necessary. Further information on the retention of personal data is available as part of the WEA Records Management, Retention and Disposal Policy.

**Purpose limitation of personal data**

The WEA will only process personal data that is necessary for a legitimate purpose that is communicated to the individual as part of the appropriate privacy notice. Personal data will not be processed further for additional purposes which are not compatible with the original purpose for processing.

**Minimisation of personal data**

The WEA will consider carefully how much personal data we need for our legitimate purpose(s). We will not collect additional personal data that is just 'nice to have'.

**Accuracy of personal data**

The WEA will keep personal data accurate - and take every reasonable step to hold information on our data subjects that is up to date.

The WEA will also be responsive to requests for personal data to be corrected. The necessary changes will be made as soon as we become aware that the data is inaccurate or out of date, and we will ensure that the updates are made across all relevant records and systems.

**Security of personal data – organisational and technical measures**

The WEA will ensure appropriate technical and organisational security measures are in place to prevent unauthorised or unlawful processing and accidental loss or destruction of or damage to personal data. This is achieved by the implementation of the following organisational measures:

- Standard background checks will be conducted on new starters as appropriate during the recruitment process and as outlined in the WEA Recruitment Policy.
- Standard employee on boarding and leavers' process, including processes for assigning access to information services based on role and removing that access when a staff member leaves.
- Mandatory GDPR compliance training with annual refresher for all staff and volunteers who handle personal data.
- Staff and volunteers who use WEA equipment and access to information must adhere to the Acceptable Use Policy.
- Staff and volunteers who use social media must adhere to the Social Media Policy when conducting WEA business.
- The WEA sets out clear guidelines and expectations for staff and volunteers in relation to the creation, maintenance, usage, storage and disposal of all types of information in our Records Management, Retention and Disposal Policy.

- As outlined in our Records Management, Retention and Disposal Policy, the WEA will ensure the following minimum standards are met when storing physical records containing personal data.
- Physical files will only be stored in WEA owned or leased premises or an appropriately accredited third-party archive facility when onsite storage is no longer possible.
- The WEA will ensure appropriate security arrangements are in place in our owned or leased premises to minimise the risk of unauthorised access to personal data. Examples may include controlled entry, intruder alarms, CCTV, staffed reception desks, procedures for locking up premises and training for staff on handling visitors etc.
- Physical files containing personal data or special category personal data will be kept locked away when not in use.
- Keys to locked areas holding physical records must be kept in a secure location with access restricted to authorised staff members only.
- Records must be accessible and retrievable as required to support business efficiency and continuity and only be accessed by those who are authorised to do so.
- Where the WEA sources the use of a third-party supplier who will have access to personal data as part of the services they provide, we will ensure a GDPR compliant contract is in place and if necessary, a non-disclosure agreement. See the WEA Use of Third-Party Services Procedure for more information.
- Where the WEA enters a partnership with a third-party organisation and personal data needs to be shared as part of that partnership, we will ensure a GDPR compliant data sharing partnership agreement is in place.
- Where the WEA processes payments from Data Subjects via a third-party payment processing company (GoCardless), the WEA maintains the standards required for PCI Compliance.
- The WEA maintains procedures for the management of Business Continuity Incidents.

**Technical measures**

- The WEA ensures that appropriate security measures are applied and maintained on all WEA owned computing equipment (including computers, mobile devices and laptops), with the minimum being password protection, encryption and antivirus software. Please see our Equipment Re-assignment and Disposal Procedure and Bring your Own Device Policy for further information.
- The WEA ensures that secure system configurations are applied, maintained and monitored on all WEA Information systems and servers. This includes appropriate firewalls, antivirus protection, administrator password controls, system updates, and email filters are in place supported by appropriate monitoring and testing activities.
- The WEA ensures that appropriate security measures are applied and

maintained on personally owned equipment that is used for the processing of WEA information. Please see our Bring Your Own Device Policy (BYOD) for further information.

- The WEA ensures that a procedure is in place to regularly back up all data held on its servers and to manage these back-ups. Please see our Data Back Up and Recovery Procedure for more information.
- The WEA ensures that access to its information systems is governed by a clear Data Access Control and Password Policy.
- The WEA ensures the security of internal communications with its stakeholders by actively working towards ensuring that all staff, tutors and volunteers hold a WEA managed Office 365 account. Please see the WEA Information Security Policy for more information.
- The WEA does not accept the use of portable storage devices (such as USB memory sticks or removable hard disks) for the transfer of personal or academic information. Please see the WEA Information Security Policy for more information.
- The WEA ensures that controls are in place for all third parties who need full or partial access to our information systems. Please see our Third-Party System Access Policy for more information.
- As the WEA takes responsibility for all the information held on its information systems, we reserve the right to undertake periodic monitoring of user activity and content to ensure that the WEA and its stakeholders are acting lawfully and within its policies.

**International transfers of personal data**

The WEA will safeguard all personal data we process by ensuring that the only international transfers of personal data are as follows:

- Transferring to European Economic Area (EEA) countries
- Transferring to the United States under the UK Extension to the EU-US Data Privacy Framework
- Transferring under “EU Model Clauses” agreement with the importing party.

Owing to the global nature of the Internet infrastructure, the information you provide to us may be transferred in transit to countries outside the EEA. These countries do not have similar protections in place regarding your personal data. Where this is the case, the WEA will take additional security steps to safeguard your data by applying end-to-end encryption; to ensure personal data is transmitted securely.

**Data incident management**

The WEA will ensure that all data incidents are reported, investigated, assessed and, if necessary, reported to the Information Commissioners Office within the legally required timeframe. The WEA will also notify data subjects affected by

a data breach if it poses a high risk to their rights and freedoms.

For more detailed information on data incident management please see our Data Incident Management Procedure.

**The rights of data subjects**

Individuals have the following legal rights in relation to their personal data:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to challenge automated decision making
- Right to object

To exercise these rights, data subjects are entitled to submit a Subject Access Request (SAR).

The WEA will provide detailed procedures and specialist staff resources to support the timely handling of SARs. For more detailed information on the process for handling SARs please see our Subject Access Requests Procedure.

**Data protection by design – Data Protection Impact Assessments (DPIA)**

The WEA will consider data protection issues as part of the design and implementation of new systems, services, products and processes that involve the processing of personal data.

The WEA will consider data protection whenever we make a change to existing systems, services, products and processes, and will periodically review existing DPIA's.

The WEA will conduct DPIA's for processing activities that could represent a risk to the rights and freedoms of data subjects, and for new systems, services, products and processes this must happen **before that processing is undertaken.**

**Freedom of Information Act**

The WEA is a public authority under the Freedom of Information Act 2000 and/or a Scottish public authority under the Freedom of Information (Scotland) Act 2002. The WEA will provide information to members of the public under the provisions of this legislation.

## 7. Adherence to this Policy

Adherence to this policy will be measured as follows:

Governance KPI measures and data protection reporting, including:

- Reporting on completed mandatory annual training
- Review of Data Protection Impact Assessments (DPIA), Record of Processing Activities (ROPA) and Information Asset Registers (IAR) to maintain personal data processing records across WEA.
- Data Incident/ Data Breach reporting
- Information rights reporting

Non-adherence to WEA policies and procedures may lead to disciplinary action.