DRAFT
Data Protection Policy

Version Number	Date of Issue	Department	Owner
1.2	17/01/2019	Information Systems	Jaimie Scully Senior Data Protection Officer

Table of Contents

1. Introduction

1.1. 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.

1.2. 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.

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

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

2. Scope

2.1. This policy applies to the whole of the WEA, and to all of its activities. It applies to all Personal Data and all other information that can reasonably be considered to 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 the registration number 2806910. In this policy references to "you" mean anyone that processes personal data for us, regardless of their employment status.

2.2. This policy applies equally to:

- The WEA in England
- The WEA in Scotland
- WEA Branches
- Members of staff, tutors, students, volunteers and members
- Service providers, partner organisations, contractors, consultants, affiliates, advisors and temporary staff engaged by the WEA

3. Key terms used in this policy

3.1. **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, credit card numbers, logon credentials, marketing preferences and data gathered from website cookies are all capable of being personal data.

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

3.3. **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'.

3.4. **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.

4. Arrangements

Data Protection Officer

4.1. The WEA employs a dedicated Data Protection Officer (DPO) as required by the General Data Protection Regulation (GDPR) as the organisation is processing personal and special category data for a high volume of data subjects on behalf of a public body.

4.2. An overview of The Data Protection Officer role is shown in section 4 (responsibilities).

4.3. 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.

Lawful basis for processing personal data and special category personal data

4.4. 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.

4.5. 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 GDPR.

Records of processing activities

4.6. The WEA will hold a record of its data processing activities within a master Data Inventory. This record will include specific information about each information asset including the purposes for processing, data sharing information, lawful basis for

processing, any joint controller details and retention period. (See Data Inventory / Mapping Procedure).

Privacy Notices

4.7. In order 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.**

4.8. 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 easily accessible form, using clear and plain language.

4.9. **All WEA Privacy Notices include:**

4.9.1. The controller's identity and contact details;
4.9.2. The Data Protection Officer's contact details;
4.9.3. What personal data is processed;
4.9.4. The purposes of the processing;
4.9.5. The lawful basis for the processing;
4.9.6. Who the personal data will be shared with;
4.9.7. Details of any international transfers of personal data;
4.9.8. The period for which personal data will be stored;
4.9.9. Details of any automated decision-making using the personal data;
4.9.10. Details of the data subject's rights and how they can exercise these;
4.9.11. Details of how to complain to the Information Commissioners Office if unsatisfied.

4.10. Links to the current privacy notices in use by the WEA are available at the end of this policy.

4.11. Any additional Privacy Notices will be developed in conjunction with the Data Protection Officer

Storage limitation of personal data

4.12. 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.
4.13. Further information on the retention of personal data is available as part of the WEA Data Retention Procedure.

Purpose limitation of personal data

4.14. 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. The personal

data will not be further processed for additional purposes which are not compatible with those purposes.

Minimisation of personal data

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

Accuracy of personal data

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

4.17. 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

4.18. The WEA will ensure appropriate technical and organisational security measures in place to prevent unauthorised or unlawful processing and accidental loss or destruction of or damage to personal data.

4.19. This is achieved by the implementation of the following measures:

Organisational Measures

4.19.1. Standard background checks undertaken as appropriate during recruitment process and outlined in the WEA Recruitment Policy.

4.19.2. 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.

4.19.3. Mandatory GDPR compliance training with annual refresher for all staff and volunteers who handle personal data.

4.19.4. WEA expectations on staff and volunteers who use WEA equipment and information services are made clear in our Acceptable Use Policy.

4.19.5. WEA expectations on staff and volunteers who use social media are made clear in our Social Media Policy.

4.19.6. The WEA sets out a clear system for the labelling, handling and disposal of all types of information in our Data Handling and Classification Procedure.

4.19.7.The WEA will ensure the following minimum standards when storing physical records containing personal data:

4.19.7.1.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.

4.19.7.2.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, manned reception desks, procedures for locking up premises and training for staff on handling visitors etc.

4.19.7.3.Physical files containing personal data or special category personal data will be kept locked away when not in use and that the keys will be kept in a secure location.

4.19.7.4.Incoming and outgoing mail will be kept locked away when not being processed and that the keys will be kept in a secure location.

4.19.7.5.Access to keys will be restricted to authorised staff members only.

4.19.7.6.More detailed instructions on how to create and maintain a secure environment for the physical storage of personal data is available in our Physical Security Procedure.

4.19.8.The WEA internally monitors levels of security by carrying out site compliance audits. Please see the WEA Data Protection Compliance Audit Procedures for more information.

4.19.9.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.

4.19.10.Where the WEA enters into partnership with third party organisation and personal data needs to be shared as part of that partnership, we will ensure a GDPR compliant partnership agreement is in place. See the WEA Data Sharing Procedure for more information.

4.19.11.Where the WEA processes payments from Data Subjects via a third party payment processing company, the WEA maintains the standards required for PCI Compliance. See the WEA Payments Processing Procedure for more information.

4.19.12.The WEA maintains procedures for the management of Business Continuity Incidents. Please see our Business Continuity Plan Incident Response Procedures and Data Incident Management Procedures for more information.

Technical Measures

4.19.13.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 for further information.

4.19.14. 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.

4.19.15. 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.

4.19.16. 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.

4.19.17. The WEA ensures that access to its information systems is governed by a clear Data Access Control and Password Policy.

4.19.18. The WEA ensures the security of internal communications with its stakeholders by ensuring that all staff, tutors and volunteers hold a WEA managed Office 365 account. Please see the WEA Information Security Policy for more information.

4.19.19. The WEA does not accept the use of portable storage devices (such as USB memory sticks or removable hard disks. Please see the WEA Information Security Policy for more information.

4.19.20. 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.

4.19.21. 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

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

4.20.1. Transferring to the European Economic Area (EEA) countries
4.20.2. Transferring to an adequate European Union (EU) country,
4.20.3. Transferring to a US Privacy Shield company.
4.20.4. Transferring under “EU Model Clauses” agreement with the importing party.

4.21. Owing to the global nature of the Internet infrastructure, the information you provide to us may be transferred in transit to countries outside the European Economic Area. These countries do not have similar protections in place regarding the protection of 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

4.22. 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.

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

The rights of data subjects

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

4.24.1. Right to be informed
4.24.2. Right of access
4.24.3. Right to rectification
4.24.4. Right to erasure
4.24.5. Right to restriction of processing
4.24.6. Right to data portability
4.24.7. Right to challenge automated decision making
4.24.8. Right to object

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

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

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

4.27. 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.

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

The WEA will conduct Data Protection Impact Assessments (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.**

4.29. For more detailed information on The DPIA Process please see our Data Protection Impact Assessment Procedure.

Freedom of Information Act

4.30. The WEA 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.

5. Links to supporting policies / procedures

Document Title	Location
Data Inventory / Mapping Procedure	https://intranet.wea.org.uk/data-protection/gdpr-policies
Student Privacy Notice	https://www.wea.org.uk/about-us/policies
Employee Privacy Notice	https://intranet.wea.org.uk/hr/policies-and-procedures
Member Privacy Notice	https://www.wea.org.uk/about-us/policies
Recruitment Privacy Notice	https://www.wea.org.uk/about-us/policies
Volunteer Privacy Notice	https://intranet.wea.org.uk/volunteers
Data Retention Procedure	https://intranet.wea.org.uk/data-protection/gdpr-policies
Recruitment Policy	https://intranet.wea.org.uk/hr/policies-and-procedures
Acceptable Use Policy	https://intranet.wea.org.uk/data-protection/gdpr-policies
Social Media Policy	https://intranet.wea.org.uk/hr/policies-and-procedures
Data Handling and Classification Procedure	https://intranet.wea.org.uk/data-protection/gdpr-policies
Physical Security of Personal Data Procedure	https://intranet.wea.org.uk/data-protection/gdpr-policies
Data Sharing Procedure	https://intranet.wea.org.uk/data-protection/gdpr-policies
Use of Third Party Services Procedure	https://intranet.wea.org.uk/data-protection/gdpr-policies
Payment Processing Procedure	https://intranet.wea.org.uk/data-protection/gdpr-policies
Business Continuity Plan and Incident Response Procedures	https://intranet.wea.org.uk/data-protection/gdpr-policies

Data Protection Compliance Audit Procedures	https://intranet.wea.org.uk/data-protection/gdpr-policies
Data Back-up and Recovery Procedure	https://intranet.wea.org.uk/data-protection/gdpr-policies
Information Security Policy	https://intranet.wea.org.uk/data-protection/gdpr-policies
Data Access Control and Password Policy	https://intranet.wea.org.uk/data-protection/gdpr-policies
Third Party System Access Policy	https://intranet.wea.org.uk/data-protection/gdpr-policies
Equipment Re-assignment and Disposal Procedure	https://intranet.wea.org.uk/data-protection/gdpr-policies
Bring Your Own Device (BYOD) Policy	https://intranet.wea.org.uk/data-protection/gdpr-policies
Data Incident Management Procedure and supporting poster on how to report a data incident	https://intranet.wea.org.uk/data-protection/gdpr-policies
Subject Access Requests Procedure	https://intranet.wea.org.uk/data-protection/gdpr-policies
Data Protection Impact Assessment Procedure	https://intranet.wea.org.uk/data-protection/gdpr-policies

6. Contact information

Policy Owner: Senior Data Protection Officer
Tel: 0300 303 3464
Email: dataprotection@wea.org.uk
Address: 10B, Josephs Well, Hanover Walk, Leeds, LS3 1AB

7. Review period

This policy will be reviewed every year by the Senior Data Protection Officer.

8. Revision history

Version Number	Date of Change	Description of Change
1.0	01/05/2018	GDPR compliant policy released in draft format (subject to further review).
1.1	09/01/2019	Review and update of Data Protection Policy. General review of all sections following additional legal advice. Approved by Senior Management Team.
1.2	17/01/2019	Responsibilities section removed following legal advice.