Workers' Educational Association

DATA PROTECTION POLICY

Summary:	This document defines the WEA's Data Protection Policy
Author:	David Morris WEA ICT Manager
Status:	Release
Version:	1.0
Date:	02nd May 2017

Contents

Contents ..... **ii**

Document Control ..... **iii**

1. Version History iii
2. Approvals iii

Introduction **1**

1. Why the WEA has a Data Protection Policy 1
2. The European Union General Data Protection Regulation 1

The WEA Data Protection Policy – Statement of Intent **3**

1. Scope 3
2. Purpose 3
3. Protection of Personal Data and other sensitive or confidential information 3
4. Commitment to Privacy 3
5. Data Protection Officer 3
6. Responsibilities 3
7. Incident Response Team 4
8. Associated Policies and Procedures 4

The WEA Data Protection Policy – Implementation **5**

1. Scope 5
2. Purpose 5
3. Protection of Personal Data and other sensitive or confidential information 6
4. Commitment to Privacy 6
5. Data Protection Officer 7
6. Responsibilities 8
   - 6.1. Responsibilities of Trustees 8
   - 6.2. Responsibilities of Chief Operating Officer 9
   - 6.3. Responsibilities of all WEA Staff 9
   - 6.4. Responsibilities of WEA Managers 9
   - 6.5. Responsibilities of Regional Education Managers for awareness and compliance by Committee Members and Volunteers 10
   - 6.6. Responsibilities of Third Party Service Providers 11
7. Incident Response Team 11
8. Associated Policies and Procedures 13

Document Control

1. Version History

Date	Version	Status	Comments
02nd May 2017	1.0	RELEASE	Status and version of final draft changed to Release Version 1.0
7 November	1.1	RELEASE	Amendment to Scope

2. Approvals

Version 1.0 of this document is approved for adoption as the WEA's Data Protection Policy.

Date	Name	Position	Signature
02/05/17	Ian Hanham	Chief Operating Office	Ian Hanham

Introduction

1. Why the WEA has a Data Protection Policy

Information is now more than ever a commodity sought, used, bought and sold in both legitimate business operations and regrettably in illegal/criminal activities too. In response to this, people increasingly want to know what information an organisation holds about them, why this was obtained, how and where it is being stored, who has access to it, what it is being used for, and how it is being disposed of.

In the course of its activities the Workers' Educational Association (WEA) uses, creates and stores information (data) which will be derived from many sources. It may exist in many forms, be stored in a number of locations, be used for a variety of purposes and have varying degrees of sensitivity. In its entirety this information is a hugely valuable and vulnerable asset which is either owned by or in the care of the organisation.

Ensuring this asset is processed and secured appropriately is both a legal responsibility and a task critical to the organisation's ability to operate.

A failure to protect and use this asset appropriately could result in significant damage to the WEA's reputation and credibility, and/or very significant financial loss (either as a direct consequence of a security breach, or in the form of fines imposed on the organisation).

By contrast, a properly structured and maintained approach to data security can simplify and introduce efficiencies in the WEA's business activities, and enhance the reputation and credibility the organisation has with its many stakeholders.

Threats to the security and integrity of the data the WEA holds can, and do, arise from any number of sources within and, outside of, the WEA. New threats appear every day, and they are increasingly subtle, sophisticated and pernicious. Risk arises from the possibility of the WEA being the victim of a malicious or illegal act, or suffering the consequence of accident or carelessness. Ultimately the WEA will have failed in its duty of care if it does not anticipate, assess and then where appropriate take action to militate against the organisation falling victim to the more likely of these events (i.e. the WEA will have demonstrated poor risk management).

In publishing a Data Protection Policy the WEA defines a framework within which the organisation can execute its legal obligations for data protection matters. It sets out the WEA's responsibilities for the Personal Data it collects, stores, uses and disposes of in a cohesive and comprehensive way.

2. The European Union General Data Protection Regulation

Data protection legislation was enacted in the European Union (EU) in 1995 and in the UK in 1998. Much has changed since then, and a few years ago the EU recognised there was a need for member states to strengthen and standardise their data protection measures. The General Data Protection Regulation (GDPR) is the result of work to achieve this goal.

The primary objectives of the GDPR are to give citizens back the control of their personal data, to simplify the regulatory environment for businesses (by establishing a common

standard across the whole of the EU), and to address concerns arising from the export of personal data to locations outside of the EU.

The EU General Data Protection Regulation (Regulation (EU) 2016/679) was adopted on the 27th April 2016. The Regulation allows organisations a two-year transition period (ending on the 25th May 2018) for achieving compliance with its requirements. As a 'Regulation' it will come in to force automatically: it does not require the government of an EU Member State to pass any enabling legislation.

Because the UK has now decided not to remain a member of the EU the GDPR may only directly apply to the UK for a short while. But, like any country wanting to trade with an EU Member State, the UK will have to prove data protection 'adequacy' to be allowed to do so. That is, UK data protection standards will have to be equivalent to the EU's GDPR. Consequently, whilst this document makes extensive reference to the Data Protection Act 1998 the requirements of the GDPR will almost certainly be adopted by the UK during 2017.

The WEA therefore needs to anticipate – and plan for – the GDPR becoming the UK's 'de facto' data protection framework.

The WEA Data Protection Policy - Statement of Intent

1. Scope

- **The WEA's Data Protection Policy applies to the whole of the WEA, and to all of its activities.**
- **The Policy applies wherever Personal Data and all other information that can reasonably be considered to be sensitive or confidential that is held or processed by the WEA.**

2. Purpose

- **The purpose of the WEA's Data Protection Policy is to define a framework within which the organisation can execute its legal obligations under the Data Protection Act 1998 ("The Act") and/or the General Data Protection Regulation (GDPR) in a cohesive and comprehensive way when collecting, storing, using and disposing of Personal Data.**

3. Protection of Personal Data and other sensitive or confidential information

- **The WEA will take appropriate technical and organisational measures to protect any Personal Data and all other information that can reasonably be considered to be sensitive or confidential that it stores or processes.**

4. Commitment to Privacy

- **The WEA commits to respecting the privacy of all individuals when holding or processing their Personal Data and all other information that can reasonably be considered to be sensitive or confidential.**

5. Data Protection Officer

- **The WEA shall appoint a Data Protection Officer (DPO). The DPO is the member of staff responsible for ensuring that the WEA is compliant with Data Protection legislation.**
- **The DPO may carry out another role within the Association but (s)he shall be accountable to the Chief Operating Officer for ensuring the WEA's use of Personal Data is compliant with the law, across the whole of the WEA.**

6. Responsibilities

The WEA will define the responsibilities it expects its Trustees, Managers, Members of Staff (including Tutors), Volunteers, Committee Members and Third-Party Service providers to have relating to Data Protection, and to observe when

using or processing Personal Data and all other information that can reasonably be considered to be sensitive or confidential.

7. Incident Response Team

- **The WEA will constitute an Incident Response Team (IRT).**
- **The IRT will consist of 'standing' members (who will be Managers responsible for critical functions within the WEA), and 'co-opted' members. 'Standing' members will participate every time the Incident Response Team is convened, 'Co-opted' team members will be identified and requested to participate where their skills or knowledge are relevant to the investigation of a particular incident, or where they are required to deputise for a 'Standing' member who is unavailable.**
- **The IRT will be accountable to the Chief Operating Officer**
- **Should there be a data security breach (actual or suspected) then the Data Protection Officer (DPO) will initiate an immediate investigation and bring the incident to the attention of the IRT (to include convening an immediate meeting of the IRT where this is considered necessary).**

8. Associated Policies and Procedures

- **The WEA will publish and maintain associated Policies and Procedures defining requirements to be observed when specific tasks are to be undertaken, or when specific circumstances apply.**
- **For the avoidance of doubt these additional Policies and Procedures should be considered to be parts of this Policy.**

The WEA Data Protection Policy - Implementation

1. Scope

The WEA's Data Protection Policy applies to the whole of the WEA, and to all of its activities. The Policy 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.

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

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, Contractors and Temporary Staff engaged by the WEA

2. Purpose

The purpose of the WEA's Data Protection Policy is to define a framework within which the organisation can execute its legal obligations under the Data Protection Act 1998 ("The Act") and/or the General Data Protection Regulation (GDPR) in a cohesive and comprehensive way when collecting, storing, using and disposing of Personal Data.

The Act lists eight Data Protection principles which the WEA must observe. In summary, those principles state:

- Personal Data must be processed fairly and lawfully.
- Personal Data must only be obtained for defined, limited and lawful purposes.
- Personal Data shall be adequate, relevant and not excessive relative to the purpose for which it was obtained.
- Personal Data must be accurate and, where necessary, kept up to date.
- Personal Data must not be kept for longer than is necessary relative to the purpose for which it was obtained.
- Personal Data shall be processed in accordance with the rights of data subjects under The Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful access to or processing of Personal Data and against accidental loss, destruction, or damage to Personal Data.

- Personal Data shall not be transferred outside the European Economic Area unless the receiving country or territory ensures adequate levels of protection for the rights and freedoms of data subjects in relation to the processing of Personal Data.

The WEA's Data Protection Policy ("The Policy") is therefore intended to ensure that:

- The WEA complies with Data Protection law, and follows good practice when processing or storing Personal Data and all other information that can reasonably be considered to be sensitive or confidential
- The WEA takes necessary action to protect the rights of those whose Personal Data is used, stored or processed by the WEA
- The WEA is open about the steps it takes to protect the rights of those whose Personal Data is used, stored or processed by the WEA
- The WEA defines arrangements the organisation must have in place to protect itself from the risks of a data breach.

3. Protection of Personal Data and other sensitive or confidential information

The WEA will take appropriate technical and organisational measures to protect Personal Data and any other sensitive or confidential information that it stores or processes. This shall include undertaking a Data Protection Impact Assessment whenever a new activity or a change to systems or procedures supporting existing activities is being contemplated.

Identifying what is (or is not) Personal Data can be a complex task. It can be as much about the context in which data is considered or processed, or about implications that may be drawn from such a context, as it is about the actual data itself.

Data means information that is processed automatically or is recorded with the intention of being processed automatically. Any data recorded as part of a manual (i.e. paper-based) filing system or with the intention that it should form part of such a filing system is also included in this definition.

Personal Data means data (processed in manual or electronic form) which relates to a living individual **who can be identified from that data** or from that data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller. It also includes any expression of opinion about an individual and any intentions of the Data Controller or any other person in respect of the individual. As examples, an individual's home address, personal (home and mobile) phone numbers and personal email address are defined as personal data.

A flowchart for determining whether information held by the WEA constitutes 'Personal Data' for the purposes of the Data Protection Act is published on the WEA Intranet

4. Commitment to Privacy

The WEA commits to respecting the privacy of all individuals when holding or processing their Personal Data. When collecting Personal Data the WEA will:

- Inform individuals why their Personal Data is being collected

- Be open and honest as to how the Association intends to use the Personal Data it collects
- Only use people's Personal Data in ways that they would reasonably expect and make sure not to do anything unlawful with it
- Not retain Personal Data longer than is reasonable and/or necessary, and dispose of it responsibly when the need for retention ends

5. Data Protection Officer

The WEA shall appoint a Data Protection Officer (DPO). The DPO is the member of staff responsible for ensuring that the WEA is compliant with Data Protection legislation. The DPO may carry out another role within the Association but (s)he shall be accountable to the Chief Operating Officer for ensuring the WEA's use of Personal Data is compliant with the law across the whole of the WEA.

The DPO is the key point of contact for staff and other stakeholders (Members, Volunteers, Trustees) in respect of Data Protection legislation and (s)he will liaise directly with the Information Commissioners' Office should there be an actual or suspected data breach.

The DPO will work with colleagues throughout the WEA to ensure that the organisation's Data Protection Policy and associated procedures are, and remain, 'fit for purpose' and that they are implemented across the whole of the organisation.

The Data Protection Officer's responsibilities specifically include:

1. Maintaining an awareness of the legal requirements of the WEA relating to its Data Protection obligations, and communicating these to WEA managers.
2. Developing, implementing and maintaining the WEA's Data Protection Policy
3. Ensuring the associated Policies and Procedures needed to support the WEA's Data Protection Policy are developed, implemented and maintained, and producing any additional 'best practice' guidance material considered necessary.
4. Providing an internal consultancy service (information and guidance) on the processing of Personal Data within the WEA.
5. Identifying training needs, designing course content and ensuring training schedules are arranged which are intended to ensure staff and volunteers are all properly prepared to fulfil their Data Protection responsibilities.
6. Ensuring the WEA's 'Data Protection' registration with The Information Commissioners' Office is maintained in terms of currency and accuracy.
7. Ensuring any Personal Data breach the WEA experiences which is likely to result in a high risk for the rights and freedoms of the individuals affected is reported to the appropriate Authorities e.g. Charity Commission, Information Commissioners' Office etc. as considered necessary or mandated by Statute. Any such report shall be made within the timescales required by those Authorities or Statutes.
8. Ensuring any security breaches experienced by the WEA and thought to be a consequence of criminal activity is reported to the Police and/or other National Security organisations.

9. Maintaining a Register of incidents brought to the attention of the WEA's Incident Response Team, and the actions taken to investigate and respond to those reports of incident.

10. The DPO will work with:
    a. The WEA's Strategic Information Systems Manager to ensure that Personal Data held in the WEA's MIS systems is only accessible to people properly authorised to use or maintain it.
    b. The WEA's HR Manager to ensure records of staff training and staff awareness of Data protection obligations are maintained.
    c. The WEA's ICT Manager ensure that appropriate arrangements are made and maintained to protect Personal Data collected by, stored in, or processed by the WEA's ICT infrastructure and generic IT services (specifically the WEA's email and files/folders held in the WEA's electronic storage facilities).
    d. Other WEA Managers to ensure that appropriate arrangements are made and maintained to protect Personal Data collected by, stored in, or processed by the WEA's HR, Finance, Education, Web (Membership, Volunteering and Marketing) and other functions including information processed and stored by both electronic and non-electronic means

       In all cases these controls are to be achieved by
       - Ensuring users are properly authenticated and uniquely identified before being granted access to data held in the WEA's systems.
       - Ensuring Role-based' limitations are implemented where required to restrict the data accessible to any particular user
       - Ensuring that systems and services the WEA uses to process or store Personal Data are configured, managed and maintained appropriately and in a timely fashion such that the WEA's obligation to observe the 'Eight Data Protection Principles' is assured (see Purpose Section of this document).

6. Responsibilities

The WEA expects its Trustees, Managers, Members of Staff (including Tutors), Volunteers, Committee Members and Third-Party Service providers to observe the obligations placed upon them by the WEA when they are using or processing Personal Data and all other information that can reasonably be considered to be sensitive or confidential.

6.1. Responsibilities of Trustees

The WEA Board of Trustees has ultimate responsibility for the strategic direction of the WEA and ensuring that the organisation complies with relevant statutory requirements (governance). For Data Protection matters this responsibility will be exercised by holding the WEA's Senior Management Team to account for the practical implementation of the requirements of this Policy across the whole of the Association.

6.2. Responsibilities of Chief Operating Officer

Within the WEA's Senior Management Team the Chief Operating Office is responsible for ensuring the requirements of this Policy are properly implemented across the whole of the Association.

6.3. Responsibilities of all WEA Staff

Individuals working for (or with) the WEA are individually responsible for complying with the requirements of this Policy and for following the instructions given in the associated Policies and Procedures published in support of it.

Any member of WEA staff could be the first to notice or become aware of a 'Data Protection' issue needing attention: they may, as examples, suspect there is a problem with a data security arrangement or provision, or they may be the recipient of a Freedom of Information request. In such circumstances the individual should report the matter promptly (and time may be of the essence) to either the Data Protection Officer or another responsible person such as their line manager so that it can be investigated or responded to. In particularly sensitive circumstances a report should be made via the procedures set out in the WEA's Public Interest Disclosure (Whistleblowing) Policy.

A number of associated Policies and Procedures sit alongside this Data Protection Policy. Staff will be guided towards those which are most relevant to them, but need to remain aware of all associated Policies and Procedures.

Each WEA employee will be required to attend Data Protection training, and confirm that they have read and understood the WEA's Data Protection Policy and the associated Policies and Procedures most relevant to them. Such confirmation and completion of the required Data Protection training must be formally recorded, either on a Form designed for this purpose or electronically on a system approved for this purpose.

New employees will be asked to confirm that they have read and understood the WEA's Data Protection Policy and the associated Policies and Procedures most relevant to them immediately after receiving their 'Data Protection' training that must be delivered to them as part of their Induction Training.

Each WEA employee will be required to attend refresher training, and re-affirm that they have read and understood the WEA's Data Protection Policy (and the associated Policies and Procedures most relevant to them) on an annual basis. Such re-affirmations and completion of the refresher training must be formally recorded, either on a Form designed for this purpose or electronically on a system approved for this purpose.

Members of Staff are advised that non-compliance with the WEA's Data Protection Policy and its associated Policies and Procedures could lead to disciplinary action being taken.

6.4. Responsibilities of WEA Managers

In addition to their responsibilities as a member of staff, WEA Managers also have responsibility for ensuring staff who report to them are aware of their duty to comply with Data Protection legislation, and to observe the requirements of this Policy and the

associated Policies and Procedures published in support of it. As a minimum, Managers shall:

- Ensure staff who report to them receive training on the requirements of the WEA's Data Protection Policy, on the Data Protection risks the WEA faces, and on the associated Policies and Procedures these staff are required to observe.

  These Policies and Procedures have been designed to ensure the WEA meets its Data Protection responsibilities and mitigates identified risks. 'Data Protection' training shall always form part of the Induction Training a new member of staff receives when they join the WEA, and additional 'refresher/update' training may be needed in support of the requirement to re-affirm at least annually that they have read and understood the WEA's Data Protection Policy and the associated Policies and Procedures relevant to them.

- Ensuring staff who report to them are properly equipped to comply with the WEA's Data Protection Policy and its associated policies and procedures.
- Arranging / facilitating audit activities arranged with the purpose of ensuring the WEA is conforming to the requirements of its Data Protection Policy.

In addition to their responsibilities as members of staff, managers are advised that they may be held accountable if staff who report to them do not comply with the WEA Data Protection Policy (including its associated Policies and Procedures) and it is shown that they have not taken appropriate action to ensure compliance by their staff.

6.5. Responsibilities of Regional Education Managers for awareness and compliance by Committee Members and Volunteers

Regional Education Managers are responsible for ensuring that all Volunteers and Branch Committee Members ("Volunteers") in their Region are aware of their responsibilities under the Data Protection Act, and ensure that the WEA Data Protection Policy and its associated Policies and Procedures are effectively communicated to the Volunteers in their Region.

With assistance from other colleagues within the WEA, this responsibility will be exercised by:

- Ensuring Volunteers in their Region receive training on the WEA's Data Protection Policy, on the Data Protection risks the WEA faces, and on any associated Policies and Procedures their Volunteers are required to observe.
- Ensuring their Volunteers are properly equipped to comply with the WEA's Data Protection Policy and its associated Procedures;
- Arranging / facilitating audit activities arranged with the purpose of ensuring the WEA is conforming to the requirements of its Data Protection Policy.

Requiring all Volunteers to attend Data Protection training, and confirm that they have read and understood the WEA's Data Protection Policy and the associated Policies and Procedures relevant to them. Such confirmation and completion of the

required data Protection training must be formally recorded, either on a Form designed for this purpose or electronically on a system approved for this purpose.

- Requiring all Volunteers to attend refresher training, and re-affirm that they have read and understood the WEA's Data Protection Policy and the associated Policies and Procedures relevant to them on an annual basis. Such re-affirmations must be formally recorded, either on a Form designed for this purpose or electronically on a system approved for this purpose.

6.6. Responsibilities of Third Party Service Providers

Certain Third Party Service Providers (e.g. external organisations the WEA has engaged or contracted or has entered in to partnership with) will act as a WEA Data Processor. They may, in the legitimate execution of the activities they are required to undertake for or with the WEA, make use of or be able to access personal data (either in electronic or non-electronic form) which ultimately the WEA is responsible for securing.

These Service Providers shall be made aware of their responsibilities as a WEA Data Processor to protect this personal data, and ensure that they and their agents (usually, but not exclusively their staff) comply with the requirements of the WEA Data Protection Policy and the associated Policies and Procedures relevant to them.

This responsibility shall be formally documented in a Contract or Service Level Agreement (SLA) between the WEA and a Service Provider, and the Contract or SLA shall also allow the WEA to conduct an audit of Service Provider compliance with these requirements on demand.

WEA Managers and staff responsible for engaging or working with Third Party Service Providers must ensure that those Service Providers are aware of, and comply with, their responsibilities as a WEA Data Processor and that contracts or SLAs between the WEA and the service provider include an obligation to comply with the requirements of the WEA Data Protection Policy.

7. Incident Response Team

The WEA will constitute an Incident Response Team (IRT) which will consist of 'standing' members and 'co-opted' members. 'Standing' members will participate every time the Incident Response Team is convened, 'Co-opted' team members will be identified and requested to participate where their skills or knowledge are relevant to the investigation of a particular incident, or where they are required to deputise for a 'Standing' member who is unavailable.

The IRT will be accountable to the Chief Operating Officer, and the 'standing' membership of the WEA's Incident Response Team will be:

- The Chief Operating Officer
- The Data Protection Officer
- The ICT Manager
- The Governance Manager
- The Head of Finance and Business Planning

Should there be a data security breach (actual or suspected) then the Data Protection Officer (DPO) will initiate an immediate investigation and bring the incident to the attention of the IRT (to include convening an immediate meeting of the IRT where this is considered necessary).

The DPO will take guidance, as appropriate, from the Information Commissioner's Office and other official bodies relevant to the circumstances of the actual or suspected breach.

The purpose of the Incident response team is (in order of priority) to:

1. Determine whether or not a data security breach has taken place.
2. Where a data security breach has taken place to make an immediate assessment of the likely extent of the breach, and identify the known, probable and possible cause and consequences of it.
3. Ensure action has – or is – being taken to prevent a continuing breach of data security and a future, repeat incidence of the breach
4. Ensure, when it is determined a reportable data security breach has occurred, that the details of the incident are reported as accurately as possible and in as timely a fashion as possible to affected individuals, and to the relevant law enforcement and statutory bodies (e.g. The Police, ICO, Charity Commission etc.).

   Notes:

   The General Data Protection Regulation (GDPR) requires the DPO report data breaches to their data protection authority unless it is unlikely to represent a risk to the rights and freedoms of the data subjects in question. This notice must be given within 72 hours of the DPO becoming aware of it unless there are exceptional circumstances, which will have to be justified.

   Where the risk to individuals is high, then those affected by the breach must also be notified. The GDPR does not specify a timescale for doing so, other than stating this must be done "without undue delay".

5. Ensure, where appropriate, that appropriate press statements are prepared, and that suitably senior WEA staff are briefed and available to respond to 'pubic interest' enquiries such as requests for a statement or comment from journalists or TV interviewers.
6. Ensure the cause(s) of the data security breach are fully investigated and make recommendations for improvements considered necessary to prevent any other data security breach occurring.

When an actual or suspected data security breach is under investigation time will be 'of the essence'. All WEA staff, Committee Members, and Volunteers are required to co-operate with, facilitate fully, and respond in a timely fashion to any request for assistance they receive from a member of the Incident Response Team.

The DPO has the authority to require any member of WEA staff, Committee Member, or Volunteer to participate as a 'Co-opted' member of the Incident Response Team where this is considered necessary to facilitate a complete and prompt investigation in to a suspected or actual data security breach.

8. Associated Policies and Procedures

The WEA will publish and maintain associated Policies and Procedures defining requirements to be observed when specific tasks are to be undertaken, or when specific circumstances apply. For the avoidance of doubt these additional Policies and Procedures should be considered to be parts of this Policy.

The associated Policies and Procedures are documented and published separately for ease of preparation and maintenance because:

1. They are likely to be of interest to functional specialists, unlike this document which is of relevance to the whole of the WEA.
2. They maybe prepared and maintained by a different person, who might be any one of the WEA's many functional specialists.
3. They can be expected to require update and amendment relatively frequently (to reflect current operational circumstances and needs) compared to the foundational statements made in this Policy document.

The associated Policies and Procedures, and a catalogue of them (including a summary of their content and their likely audience) are published on the WEA Intranet.