Llywodraeth Cymru
Welsh Government

www.wales.gov.uk

Welsh European Funding Office

European Structural Funds Programmes 2007-2013

Guidance

Management and Retention of Records

Version 2

August 2012

UNDEB EWROPEAIDD
EUROPEAN UNION

Llywodraeth Cymru
Welsh Government

Key Points

- Project financial records and supporting documents must be retained until WEFO advises that the retention period has ended.
- Records can be electronic/ digital, micro-fiche or paper.
- Records that are not the original version, e.g. a photocopy or a scanned image, must conform to the certification process described in this guidance.
- Organisations retaining records electronically/ digitally must be satisfied that their IT systems adhere to relevant computer security standards so that the authenticity of the records is assured and can be relied upon for audit and legal purposes in the UK.

1. Introduction

Records relating to EU Structural Funds projects need to be managed effectively so that WEFO and auditors can access project records for a lengthy period of time as set out by the European Commission (EC) – potentially at least 17 years for projects that started in 2007/ 2008.

The EC offers a range of document retention options, however, the lengthy retention period means that it is important to carefully consider the practical issues and risks - such as physical damage or technological obsolescence - before project managers decide on the most suitable option for their organisation.

The inability to retrieve documents, or to produce them in an authentic and reliable form, will mean that the grant funds become ineligible and would need to be repaid.

This guidance outlines the **minimum requirements** of WEFO and the EC so that organisations can decide on the best arrangements for their individual circumstances. Background information, best practice advice and frequently asked questions are also provided to help implement the guidance.

The information and advice in this guidance note relates solely to the requirements of the **Welsh Structural Funds programmes 2007-2013** and not to earlier programmes. Similarly, it does not aim to explain or substitute any of the wider records management responsibilities that may apply to a particular organisation, such as Public Records legislation, Freedom of Information, Data Protection, The National Archives, HMRC, Companies House etc.

2. Fundamental Principles

EC legislation[1] requires WEFO to ensure that all supporting documents relating to expenditure are kept available for three years following the formal closure of the Operational Programme that funded the expenditure.

Therefore, projects must retain all records until WEFO confirm that this period has expired. This date will be notified on the WEFO website. Based on previous experience of programme closure, WEFO anticipates that this point will not arrive until **at least 2024**.

EC Regulations state that supporting documents must be either originals (paper) or versions certified to be in conformity with the orignial[2] when held on commonly accepted 'data carriers'. The EC confirms that the following are commonly accepted data carriers:

- photocopy (of an original paper document)
- electronic version (of an original paper document), i.e. scanned/ digitised images
- microfiche (of an original paper document)

These versions are subject to a certification process - and for photocopies, a certification declaration - as set out by WEFO (described in section 4 below).

Records and documents that are created/ received and maintained only in electronic format are also accepted but only when the computer systems are secure and therefore provide assurance on the authenticity of the records. The EC Regulation[1] requires these computer systems to meet any 'accepted security standards' needed to comply with UK legal requirements or to be relied upon for audit purposes.

To clarify, these electronic versions are those that are created, processed, and stored in digital/ electronic format and have never been in paper form. This may be presented on-screen as a document/ e-form (such as e-invoices or e-timesheets) or can be primary records held in a database, spreadsheet, or business application etc. Sometimes these are referred to as '*born digital*' records or documents. This is discussed further in section 4 below.

Please see **Annex B** for details of the types of project records that must be retained. Projects should also refer to the retention requirements specified in the WEFO grant offer letter, which may include additional requirements, special conditions, State Aid requirements etc.

State Aid
Project sponsors also need to consider any additional requirements (including extended retention periods) that may be required relating to projects involving an element of State Aid – the record retention period is normally **10 years** from the date on which the last individual aid was granted.

This period could therefore extend **beyond** the period generally applicable to projects (three years following the formal closure of the Operational Programme) and therefore records relating to aid must still be retained until the State Aid record retention period has elapsed.

Project sponsors should check with WEFO if they are unsure of these requirements.

3. Retention and Retrieval

Retention periods
Regardless of the record retention format (paper originals, paper copies, digitised documents, electronic records), the fundamental consideration is that such records are indexed, filed, and stored to enable efficient retrieval at relatively short notice at any time until 2024 (or beyond). To illustrate the importance of this, European auditors only need to provide 10 working days notice to audit project records[4].

This means, for example, that records retained electronically are only compliant if capable of retrieval until 2024 or later. When deciding on how to retain documents, Project Managers will therefore want to consider practical issues and organisational risks such as:

- Technological obsolescence/ digital continuity (new hardware, new software, loss of staff expertise to operate legacy systems);
- Physical damage and deterioration over time;
- Exposure to loss or theft;
- Ability to transfer records to another organisation if an organisation ceases to exist (time limited entities, corporate failure etc.); and
- Personnel continuity (will new staff members be able to access records efficiently if former project staff have left the team or organisation?).

Responsibilities for retaining records
WEFO requires all lead project sponsors to maintain an up-to-date record that identifies and locates all organisations that hold supporting records for the project (this is required by EC Regulations[5]).

The contractual requirement for adequate document retention is passed in the first instance to the **lead project sponsor** via the WEFO grant offer letter –

this means that grant funds could be recovered by WEFO/ EC if the requirements are not met by any organisation holding records for the project.

However, in practice a number of other bodies may be involved in managing or delivering a project and may therefore be creating and holding project records e.g.

- Joint sponsors;
- Delivery partners (procured or non-procured);
- Procured contractors also providing match-funding support; and
- Employers of ESF participants.

Lead sponsors must therefore consider how the document management and retention requirements will be met by all these organisations, including any contractual/ legal liabilities relating to any subsequent repayment of grant funds to WEFO/EC. Alternatively, organisations may want to consider whether documents should be transferred to the lead sponsor for management and retention.

It is for the lead project sponsor to decide on the method and formality of how they convey document management expectations to its partners. However, it must be remembered that WEFO will only ask the lead sponsor to repay any irregular expenditure - even if a document retention issue arises at a partner organisation. Therefore lead sponsors should carefully consider how responsibilities are allocated from the inception of the project.

4. Document Retention Options

Options are outlined below for consideration by Project Managers. Important factors to consider will include:

- Storage space and costs;
- Each organisation's policy/ risk appetite regarding the legal admissibility of copies/ scans in UK civil courts (see **Annex C**);
- Whether 'originals' will be retained as a back-up or destroyed when a copy or scan is created?; and
- Convenience, access, ease of retrieval for current and future staff.

If projects receive more than one 'original' document (e.g. postal bank statement and a PDF electronic bank statement) then either version can be retained if it meets the requirements outlined below.

OPTION 1 - Original (paper)

This is a simple option but can be cumbersome and may have significant physical storage implications. Physical damage is a risk and the ability to retrieve documents quickly can be challenging, particularly if stored off-site.

Records will need to be clearly labelled and/or filed separately to normal business records so that each organisation holding records complies with the lengthy retention period.

No 'certification process' is required for original paper records.

OPTION 2 - Paper copy (photocopy of original paper document)

This must be the first photocopy of an original and not a 'copy of a copy'. Both sides of the original document must be copied if applicable.

The copy must be certified using the certification process outlined in the section below.

WEFO Certification Process: PHOTOCOPIES

The photocopied document (or batch of documents – see below) must contain a **certification statement**.

If one document contains multiple pages then the first page should be certified and the number of attached pages clearly indicated on the front page (alternatively, each page could be certified).

The certification declaration must be annotated on, or appended to, the copy. The original document does not need to be marked (in practice, the original will be returned to its owner or destroyed).

The certification statement must be **signed** and **dated** by an employee who can vouch that the copy is a true replica image of the original.

The certification statement is added at the time that the copy is made, or very shortly afterwards, so that the signatory can recall seeing the original and therefore confirm that the copy is satisfactory.

The 'certification statement' can be chosen by each organisation but must, at least, contain the following:

- Signature

- Date

- 'True copy', 'certified copy', 'certified' [*or similar phrase to signify what the signature and date represents*]

It is recommended, but not mandatory, that the certification statement also includes the printed name/ position of the signatory or other unique reference (such as employee/ payroll number) so that future project staff and/or auditors are able to easily identify the signatory if required.

The following is an example of a compliant certification statement:

I certify that this is a true copy of the original document

SIGNATURE:

DATE:

*PRINTED NAME/ POSITION IN ORGANISATION [**optional**]:*

*NAME OF ORGANISTAION [**optional**]:*

*NUMBER OF PAGES CERTIFIED IN THIS DOCUMENT [**if applicable**]:*

Batch Certifications

If considered more efficient, a single certification declaration can be used to certify a batch of documents. The certification statement **must** include:

- a unique batch reference number/ code to identify the batch
- the number of documents – and pages if individual documents contain more than one page – included in the certified batch
- the references/ numbers of each of the documents included in the batch. If the documents are not already referenced/ numbered, then references/ numbers should be added to each document prior to batch certification

OPTION 3 – Scan an original paper document (digitised documents)

Scanning of original paper records can be used if the WEFO certification process is followed (see below).

Scanned documents must be a true representation of the original document (a replica image, including the reverse of the document if applicable) and must not be condensed, cropped etc. Any alterations made to the scanned image must be logged in an audit trail and presentational changes (contrast, brightness, rotation, zoom etc.) must not permanently replace the original image.

The process and procedures followed are the key considerations - not the particular technology being used. The important point here is that the EC regulations (and WEFO) does not impose any higher burden beyond standard UK legal and audit requirements (see **Annex C** and **D**) other than the requirement to comply with the certification process outlined below.

WEFO Certification Process: SCANNED/ DIGITISED DOCUMENTS

CHECKLIST FOR A COMPLIANT CERTIFICATION PROCESS

- Are scanning processes and procedures documented and up-to-date?
- Does the scanning process include a quality control check (performed at the time of the scanning) to inspect the image and check that it is a true representation of the original document?
- Does the scanning process provide an opportunity to reject the image and request a rescan?
- Does the scanning process include a requirement to mark photocopies so that it is clear that the scanned image is not a scan of an original (and is not therefore acceptable for EU project records)?
- Does the system contain an automated audit trail/ system log to record the date/ time of the scan, any alterations made since first scanned (if such alterations are permitted by the system) and available for inspection by auditors until at least 2024?

Note 1

A written/ recorded 'certification declaration (as used in photocopy certifications) **is not required** because the above certification process achieves the same purpose. The acceptance of the scanned image by the scanning officer is deemed to be the certification. Some scanning and workflow systems digitally 'endorse' documents or batch headers (bar codes, watermarks, date/ time electronic stamps etc.) as evidence of the document successfully completing the scanning process but this is not an essential requirement provided that the scanning process includes the essential requirements described above.

Note 2

It will be a decision for each auditor/ inspection officer to decide the extent of checking compliance with the above requirements and, in practice, this could be a combination of a review of process and procedure manuals; observation of the scanning process in operation; examination of system logs/ audit trails; and/or accepting scanned images at face value in the absence of indications that the above measures have not been followed.

OPTION 4 - Original (electronic records and documents)

In practice, this means e-mails, word processing files, spreadsheet files, database records, electronic invoices received from suppliers, electronic data interchange etc.

The terms ‘document’ and ‘records’ can be used interchangeably in this context (in the sense that a document is information stored in a particular media format).

Where documents are created/ transmitted/ filed in electronic version only, they are, effectively, the ‘original’ and therefore **do not need to be ‘certified’**.

As with the scanning process in Option 3 above, the computer system must maintain an audit trail/ system log that would show any modifications to the records or documents (and this log must be capable of inspection until 2024 or later).

However, to use this option the EC also specifies that the computer system used must meet accepted security standards.

‘Accepted Security Standards’

The EC require the above computer systems to meet accepted security standards to ensure that the records held comply with national legal requirements and can be relied on for audit purposes.

There is no universally ‘accepted’ or mandatory security standard in the UK and therefore each organisation can decide on the appropriate security arrangements for their computer systems.

Despite the absence of a single accepted security standard, the intention of the EC Regulation must still be followed – i.e. computer systems must be sufficiently secure so as to protect the authenticity of the records (and demonstrate this if necessary) and be relied on for audit purposes and/ or UK legal requirements.

To help project sponsors, WEFO considers that the three sources outlined in Annex E are authoritative, commonly used standards/ sources of guidance that can be used as a reference point to provide assurance about the adequacy of security standards.

The key aim is that information contains the following four characteristics of an **‘authoritative record’:**

AUTHENTIC

- Is the document/ record what it purports to be?
- Was the document/ record created or sent by the person purported to have created or sent it?

- Was the document/ record created or sent at the time purported?

RELIABILE
- Can the document/ record be depended on and its contents trusted as a full and accurate representation of the transactions, activities or facts to which it claims to represent?

INTEGRITY
- Is the document/ record complete and unaltered?

USEABILITY
- Can the document/ record be located, retrieved, presented and interpreted?

An **automated audit trail/ system log must therefore be maintained** to enable the demonstration of the above four characteristics if required and to support legal admissibility. This log must be available for inspection to 2024 or beyond. This log must register any changes made to the electronic records unless it can be demonstrated that the file format is incapable of being edited - although, an automated log of the date/ time that the record was created or scanned is always required.

Computer systems must maintain the **content** of the record that would have existed when the record was first received or created e.g. not summarised, condensed or aggregated.

Important Note
Each organisation that chooses to retain records electronically/ digitally must be able to explain and demonstrate (if requested by WEFO and/ or auditors) how their IS/ IT systems adhere to the above requirements. Structural Funds audits and inspections are not designed to be computer-security compliance audits and therefore, in practice, records will usually be accepted at face value with auditors/ inspectors applying their professional judgement to identify any indications that a record is not authentic or that organisations are not aware of, or not aiming to follow, accepted security standards. Similarly, a successful audit or inspection must not be interpreted as providing assurance that computer systems are compliant with computer security standards.

OPTION 5 - Paper version of electronic records/ documents

Some electronic documents and records can be printed via an integrated 'print' option in the software application – e.g. e-invoices received by e-mail as protected PDF documents, PDF bank statements created by the online bank website application, or other PDF primary documents held within - or created by - a secure system with a hard-copy print option.

If preferred, these documents can be printed and retained as hard-copy records. The printed version **must be certified** as outlined in the certification process for photocopies (above).

Printed ‘screen prints’/ ‘screen dumps’ (copying screen images and pasting them into another application such as Microsoft Word and then printing) are **not acceptable** as the image will not be an exact replica of the ‘original’ and there is an insufficient audit trail to demonstrate that the image has not been modified prior to printing. Screen-prints however may be requested by auditors/ inspection teams to evidence their checks.

5. Personal Data and Information Security

When handling personal or sensitive data, this must be done in accordance with recognised information security requirements and applicable legislation such as the Data Protection Act, including the use of data encryption when transmitting sensitive personal data to other organisations.

For further information go to the Information Commissioners Office website www.ico.gov.uk.

End notes

[1] European Council Regulation EC 1083/2006, Article 90(1)
[2] EC 1083/2006, Article 90(3)
[3] EC 1828/2006, Article 19
[4] EC 1083/2006, Article 72
[5] EC 1828/2006, Article 19(1)
[6] EC 1828/2006, Article 19(2)

ANNEX A – Sources of Further Guidance

Document Scanning: Guide to Scanning Business Documents, British Standards Institute DISC PD 0016, ISBN 0 580 33176 8

ISO 15489-1, Information and documentation – Records Management

Planning and Implementing Electronic Records Management, Kelvin Smith, 2007, Facet Publishing ISBN 978-1-85604-615-2

Evidential Weight and Legal Admissibility of Information Stored Electronically: Code of Practice for the Implementation of BS 10008, British Standards Institute, 2008, ISBN 978 0 580 63945 6

Lord Chancellors Code (s8.3, Lord Chancellors Code of Practice on the management of records issued under section 47 of the Freedom of Information Act 2000)

Civil Evidence Act 1995, S8 and S9 (Business Records)

Information Management Codes of Practice (various), The National Archives

ANNEX B - What records should be retained?

As a minimum, the following must be retained:

- **Financial records**: e.g. receipted invoices, payments, bank statements, credit card statements, evidence of match funding, staff time-sheets, salary records, bank records and other supporting accounting documentation to identify all incurred and paid-out expenditure claimed on a project. Apportionment methodologies and calculations, including WEFO approval correspondence where appropriate, for costs covering more than one project, indirect costs, and outputs/ indicators. Records related to revenue/ income generated from project activities must also be retained;
- **Publicity**: evidence of the activity undertaken to publicise ERDF/ ESF support and comply with regulatory requirements e.g. plaques, press cuttings, press releases, advertisements, photographs and marketing materials;
- **Applications and payment claims**: copies of these, together with all working papers relating to their compilation e.g. progress reports and transaction lists that must accompany claims;
- **Contracts**: full evidence of any tendering exercise e.g. bidding process, selection criteria, justification for the appointment of the successful contractor and sector to which successful contractor relates, exchanges of correspondence offering and accepting contracts, tender report, details of tenders, sources of match funding as a result of a procurement exercise;
- **Project activity**: effective recording systems for tracking and evaluating progress of projects i.e. details of outputs achieved, beneficiary application forms/ eligibility;
- **Records of project/ management/ board meetings** and their decisions relating to the project;
- Details of support and aftercare provided to approved projects;
- All related paperwork and files in respect of approved projects i.e. all correspondence generated from the acceptance of an application for appraisal, through to approval and post approval; and
- Simplified cost options: full audit trail of expenditure/ documentation used to establish the methodology.

The above list is only a guide to requirements and is not exhaustive. Project sponsors and partners are responsible for ensuring that they retain all the necessary documentation.

ANNEX C – Legal admissibility issues

Original paper documents are not the only admissible evidence in UK civil courts – electronic records, photocopies, and digitised images can be acceptable if their integrity can be satisfactorily demonstrated. Absolute legal certainty of admissibility is not possible but adherence to best practices such as BSI Code of Practice (see **Annex A**) minimises the risk of a civil court rejecting the document.

At the time of preparing a document to be submitted as court evidence - and not at the time of the document was copied - a suitably senior member of staff must be able to certify the document as a true record of the original paper document and confirm that the original document has been destroyed. Record management policies and procedures must therefore be sufficient for a staff member to be able to make such a declaration in good faith.

It is worth noting that HMRC and Companies House both accept electronic records/ images of business records with the same validity as original records.

The Civil Evidence Act 1995 also includes provisions regarding the acceptance of business records other than original paper copies.

Each organisation holding EU Structural Fund records/ documents must decide on their approach to legal admissibility issues, assessing the likelihood of a legal dispute about the authenticity of particular records and the potential impact, if any.

WEFO (and the EC) does not add any additional standards or requirements in respect of legal admissibility beyond the normal considerations that each organisation already takes for managing routine business records.

ANNEX D - Audits and Verifications

Arrangements for Audits and Inspections

Records must be available for inspection by auditors and WEFO[6], including Reporting Accountants undertaking annual/ final certification checks as part of WEFO's verification processes. This can be 'on-screen' inspections (electronic records) or hard-copy records. In addition, projects may be asked to provide selected extracts or copies for the auditor's working files to evidence the checks performed for quality assurance purposes[6].

If selected for audit or inspection, Project Managers should advise WEFO/ auditors of the location of records (including arranging access to computer systems for on-screen inspections) so that arrangements can be put in place to visit the appropriate location or, if preferred, transfer the records to another location for inspection.

Audit trails will need to contain sufficient and necessary information to provide evidence of the authenticity of stored documents, including details of any changes to them.

It should be noted however that Structural Funds audit and inspection bodies (including EC and the European Court of Auditors) do not routinely perform specialist IT/ computer system audits when verifying project records and will not test compliance with the all the requirements of a particular standard.

Similarly, acceptance of records by auditors should not be interpreted as confirming ISO/ BSI/ MoReq2 compliance. Declarations of compliance with the BSI code are voluntary self-certification rather than needing an external compliance assessment. The real test of compliance/ conformity is when a legal or audit challenge arises and an evidence to demonstrate compliance with the relevant codes would be needed.

Acceptance of copies, scans, and electronic information

International Auditing Standards (ISA 500, ISA 240) do not prohibit copies, scans or electronic records as being acceptable audit evidence but acknowledge that they may be less reliable than (paper) originals and therefore professional scepticism is required, together with consideration of potential fraud indicators or any other reason to believe that a document may not be authentic, or may have been modified without that modification having been disclosed to the auditor.

What will auditors/ verifications officers expect to see?

PHOTOCOPIES

- Each document (or batch) contains a compliant certification declaration (see Section 4 above).
- The document appears complete, unaltered and undamaged.

- If batch certifications have been used – each document must have a reference/ code to enable matching to the associated batch certification statement.

DIGITISED/ SCANNED IMAGES

- See checklist questions in Section 4 (Option 3)

ELECTRONIC RECORDS/ E-INVOICES/ ELECTRONIC FILES

- The auditor will use their professional judgement and knowledge of the organisation/ project to determine the extent of checks they undertake to ensure that the principles of Section 4 have been followed. This could potentially involve a review of system descriptions/ manuals; examination of system logs/ audit trails; and/or accepting the electronic records in good faith in the absence of indications that the key measures have not been followed. In summary, the requirements that may be tested are:
  - The system and processes used to store records must have been designed with reference to common security standards/ functional requirements as outlined in the sources mentioned in Section 4 (ISO, BSI, MoReq2) or similar authoritative source of IT security standards such as COBIT (Control Objectives for Information and Related Technologies, Information Systems Audit and Control Association).
  - Organisations must be able to produce policies, procedures, or other internal records to demonstrate that system was designed to comply with such security standards.
  - The records/ forms must be capable of being retrieved until 2024 or beyond.
  - The records/ forms must retain the complete content that would have been in place at the time of creation and must not be summarised, aggregated, or converted to a less-detailed format in any other way.
  - An automated audit trail/log is created to note the date/ time of creation and any subsequent modifications to the records. This audit trail must be capable of being shown to auditors/ inspections staff until 2024 or beyond.

ANNEX E - Computer Security Standards

WEFO considers that the following three sources outlined are authoritative, commonly used, well-established standards/ requirements that project sponsors can use as a reference point to provide assurance about the adequacy of their compute security systems.

The three sources share common fundamental requirements and this guidance note signposts project sponsors to the key elements.

- **ISO 15489** is commonly regarded (including by The UK National Archives) as an authoritative records management text. The Welsh Government designs its own core IT systems to comply with this standard.

- **BSI 10008** (2008) British Standards Institute, Code of Practice on the Legal Admissibility and Evidential Weight of Information Stored Electronically. The code also draws upon ISO 15489 requirements.

- **MoReq2** (Model Requirements for the Management of Electronic Records 2008). The National Archives endorses and participates in this EU initiative, which incorporates and harmonises all or part of national standards across the participating European Member States. MoReq2 draws significantly on ISO / BSI requirements and the UK National Archives guidance

ANNEX F - Frequently Asked Questions

Q: Are e-invoices acceptable as project records?
A: Yes. An organisation receiving an e-invoice from a supplier or partner has two options:

- Print the document and retain a certified paper copy (Section 4, Option 5)
- Retain in electronic format (PDF/ TIF/ JPEG etc.) if the computer system meets accepted security standards (Section 4, Option 4)

Q: Can WEFO pre-approve/ quality assure computer security standards or scanning systems?
A: No. The adequacy of records management systems depends on both the design and implementation of processes and procedures over time. Each organisation holding records is responsible for ensuring records are retained in an acceptable format for the required period of time. This guidance note explains the meaning of 'acceptable format'.

Similarly, WEFO is unable to determine the nature or extent of audit work that may be undertaken by EC auditors (or the European Court of Auditors) to test the computer security standards or scanning/ certification processes. Therefore, each organisation must satisfy itself that it has maintained authoritative records and complied with the specific requirements of this guidance note such as automated system logs, documented processes, and quality control of scanned documents.

Q: Do project records need to be transferred to WEFO?
A: This may be required upon the closure of a sole project sponsor (cease trading etc.). If the lead sponsor merges, or is taken over, by another organisation – no change/ continue to retain records (new organisation inherits legal obligations to retain records or repay EU funding). If other partners close – joint sponsors/ delivery agents etc. – transfer records to lead sponsor.

Q: Are the additional costs of storage an eligible project cost?
A: Yes, they can be an eligible cost where genuinely additional and necessary (same principle as auditor certificate costs or project manager's salary – part of essential management and control costs of a project). This principle could also extend to, for example, the cost of software licences to retain electronic records until 2024 or later.

To be eligible, it must be clear that the records would not have to be retained by the organisation were it not for WEFO/ EC retention requirements. Only costs relating to the period beyond the organisations standard retention period will be considered (up to the WEFO/EC retention period).

Project sponsors will also need to budget to co-finance such costs and obtain agreement for such costs to be included in agreed spending profiles from their WEFO Project Development Officer.

From a practical perspective, such costs will need to be incurred and paid out prior to the final project claim even though the period of storage/ licensing will relate to future years.

Q: Are online bank statements acceptable?
A: Screen prints (certified or not) are not a true copy of the original. Only a photocopy or scan of the paper (postal) statement would be a true copy. Project sponsors are also unable to retain as electronic records because the on-screen information is the records of the bank and not the customer (the project sponsor). The following options are therefore available:

- Option 1: Auditors/ verifications teams can inspect the online webpage (live) as evidence of defrayment of costs for the purpose of checking a particular claim. However, longer term document retention is inadequate and would need to be addressed.
- Option 2: Ask the bank for paper (postal) statements and retain them as originals (or scan them). Bank charges for this purpose can be claimed as eligible costs (an additional cost directly relevant to management of a project).
- Option 3: Some online bank websites allow PDF statements to be created (they look similar to a postal statement). The PDF 'document properties' will contain document creation date /time and will not allow any changes. Therefore, this can be retained as an electronic record (original is electronic/ never been paper – no 'certification' needed) or could be printed and certified as a true copy (of the electronic version) and retained as paper copy.

Q: What is WEFO's view on the use of electronic signatures/ digital signatures for project financial records and participant records?
A: Images/ pictures/ bit-maps of a 'pen and ink' signature are usually presentational only and not a secure authentication system (no evidence that the signatory was aware of the use of their signature on a particular form).

Advanced electronic signatures (often called 'digital signatures') involve inputting a unique code/ key into a device or application to approve a transaction or authenticate the identity of the sender. Digital/ electronic certificates are issued (and revoked when necessary) to each individual to enable its use. Advanced electronic signatures are permitted by the EC (see EC directive 1999/93/EC) and can be used as an alternative to ink signatures.

Before starting to use such systems, project sponsors should contact WEFO Regulations & Compliance Branch to discuss the audit trail that will be available to demonstrate approval of key documents. This is only necessary for documents/ forms that WEFO require to be approved, such as forms completed by participants or staff timesheet forms.

VERSION HISTORY

Version	Date published	Summary of changes	Author/ WEFO Contact
1	May 2010	[First guidance note issued]	n/a
2	August 2012	• Additional guidance on practical implementation of requirements. • Additional guidance the minimum computer security standards required for electronic records/ documents (to support the use of e-invoices, electronic transactions etc.) • Removal of certification statements for compliant scanning processes. • More flexibility on certification statements on paper copies. • New FAQ section. • New annex on legal admissibility. • New annex on computer security standards • New annex on audit requirements.	Dean Langley (Tel 0300 062 8242)