



Digital Evidence for Internally Assessed HN and VQ Units: Principles and Guidance

First published: February 2017

Publication code: AA 7373

Published by the Scottish Qualifications Authority, The Optima Building,
58 Robertson Street, Glasgow G2 8DQ Lowden, 24 Wester Shawfair, Dalkeith,
Midlothian EH22 1FD

www.sqa.org.uk

The information in this publication may be reproduced in support of SQA qualifications. If it is reproduced, SQA should be clearly acknowledged as the source. If it is to be used for any other purpose, then written permission must be obtained from SQA. It must not be reproduced for trade or commercial purposes.

© Scottish Qualifications Authority 2017

Contents

Introduction	1
Producing digital evidence	2
Security	4
Training and support	5
Verification	5
Appendix: Checklists	7

Introduction

This Principles and Guidance document is intended to support and inform UK-based SQA co-ordinators, quality managers and centre staff delivering Higher National (HN) and vocational qualifications who would like to present digital evidence for internal and external verification. It builds on the guidance already contained in our [Guide to Visiting HN and Vocational Qualification Verification for Centres](#) and aims to encourage good practice by reflecting on the approaches that are already being used in some centres.

This is a live document that will be updated over time as we see the volume of digital evidence increase. Any feedback we receive on use of this document will help us ensure that future versions are as helpful as possible. Please send any feedback to operationshmvq@sqa.org.uk

Background

In 2015, we carried out a pilot study with a small number of centres to test the feasibility of verifying digital assessment evidence as part of our quality assurance activity. The study proved to be very successful and a number of recommendations were made, including the development of structured principles and guidance for centres on storing and accessing digital evidence. We have also received requests from centres to produce guidance on this subject, reflecting the fact that learners are increasingly generating assessment evidence digitally.

[SQA's 2015–18 Corporate Plan](#) sets out SQA's vision to '*...digitally transform our organisation to offer customers better service by delivering efficient, scalable and new enabling approaches*'.

We are increasingly accepting digital evidence as it becomes more common in our centres and we aim to further encourage the transition from paper to electronic capture of assessment evidence.

What is digital evidence?

Digital evidence is any material which has been captured and gathered digitally and is presented in its digital format as evidence for one of our qualifications. Examples of digital evidence include word-processed documents, spreadsheets and presentations, audio and video files.

Some evidence can be produced digitally but be presented in a non-digital format, such as a word-processed document that has been printed, while other evidence, such as audio and video files, can only exist digitally. Online assessment systems also generate digital evidence.

Producing digital evidence

Principle 1: SQA's principles of assessment and quality assurance processes must be adhered to regardless of the format of the evidence.

These principles state that the assessment should be valid, reliable, practicable, equitable and fair.

Ensuring the assessment is valid:

- ◆ Get to know the units
- ◆ Create an assessment plan
- ◆ Consider the candidate
- ◆ Choose the appropriate assessment method(s)
- ◆ Develop the assessment
- ◆ Define the evidence for the assessment

Ensuring the assessment is reliable:

- ◆ Check the assessment and marks scheme
- ◆ Assess the candidate
- ◆ Provide reasonable support
- ◆ Judge the evidence
- ◆ Check the consistency of assessment judgements
- ◆ Record your assessment decisions
- ◆ Record your final assessment result

Reliability can be developed by consistent use of aids such as checklists, with space for the assessor to reference evidence against the outcome and/or standard.

Ensuring the evidence is practicable

A valid and reliable assessment may not be practicable due to the resources or time required to carry it out efficiently and effectively. You should consider the demands on resources and time, and plan carefully to ensure successful outcomes.

Ensuring the evidence is equitable and fair

Consider these questions to ensure that your assessments are equitable and fair:

- ◆ Does the assessment offer all candidates an equal opportunity to demonstrate their attainment?
- ◆ Are the scenarios or contexts in the assessment open and comprehensible to all candidates?
- ◆ Could any part of the assessment or the assessment itself have an adverse impact on disabled candidates or any other groups?
- ◆ Does any illustrative material reflect an inclusive view of society which promotes equality?

It is the responsibility of centres to ensure that, where digital evidence is being used, the evidence submitted by learners meets the requirements of the relevant unit specifications and, if applicable, any assessment strategies.

SQA's [Guide to Assessment](#) should be read and used in conjunction with our wider guidance and support for assessment and quality assurance.

Principle 2: The systems selected for retention of learner evidence should not contain any features which might adversely affect end-users.

When learners access IT-based systems — eg virtual learning environments (VLEs) and e-portfolios — to support their assessment for an SQA qualification, it is your centre's responsibility to ensure that:

- ◆ there is no potential for the technical solution to cause the learner any harm
- ◆ the systems are sufficiently secure and no unauthorised access to the learners' personal details is possible

Use of personal social media accounts, such as Facebook and YouTube, for gathering assessment evidence should be avoided. 'Closed' groups on certain popular social media platforms can be easily compromised without the need for sophisticated hacking.

Centres can create their own secure YouTube account for uploading video evidence and may have facilities within their VLEs which provide learners with a social media that is similar to Facebook. It is SQA's preference that VLEs and e-portfolios are used for these purposes and that the use of social media platforms is avoided.

Take care to ensure that learners' use of IT-based systems protects their legal rights under the Equality Act 2010. Some disabled learners or learners with additional support needs may require additional training or appropriate reasonable adjustments/assessment arrangements such as the use of assistive technologies, including text/screen readers or voice recognition software.

More information on reasonable adjustments and assessment arrangements can be found on SQA's Assessment Arrangements web pages at www.sqa.org.uk/assessmentarrangements.

Further helpful information on assistive technologies can be found on CALL Scotland's website at <http://www.callscotland.org.uk>.

Security

Principle 3: Evidence created digitally should be stored under secure conditions.

Take care to ensure that assessment evidence:

- ◆ has been created by the learner who is claiming ownership of the evidence and that authentication can be provided, as it would be for non-digital evidence
- ◆ is received securely by the appropriate designated centre staff
- ◆ cannot be altered by others — learners must be able to protect/lock their evidence before they submit it
- ◆ is stored securely in a restricted access file throughout assessment and until the completion of the assessment, quality assurance and appeals processes
- ◆ is of a quality that allows verifiers to be certain of the origin of the evidence

For further guidance on the secure storage of evidence, please see our tables for [evidence retention requirements](#) and [retention of candidate assessment records](#).

Principle 4: Data security policies should be in place and should cover digital assessment evidence.

It is **very important** that centres comply with Data Protection legislation and have documented policies in place regarding the secure handling of digital materials.

Points to consider:

- ◆ Does your centre have a password reset policy?
- ◆ Does your centre have a password format policy?
- ◆ Does your centre have a policy on the use of IT systems, which mentions the need for good IT etiquette?
- ◆ Does your centre have processes in place to detect and manage plagiarism?
- ◆ Does your centre have a policy on adherence to copyright requirements?
- ◆ Does your centre have a system backup policy with details of storage of backup media?
- ◆ Do the systems within your centre have a firewall in place?
- ◆ Does your centre have a data retention policy in line with SQA guidance?
- ◆ Has your centre implemented all of the above?

Principle 5: Systems and resources should be in place to allow for secure storage and management of digital evidence.

Centres are free to select from a range of IT systems for storage and management of digital evidence. With the exception of the downtime necessary for backups and system updates to be run, wherever possible access to systems should be unrestricted, mobile friendly and accessible from outside the centre. Where an assessment takes place at a specific date and time, access should be restricted as required.

Systems should allow for materials that are generated by learners, and saved in commonly used formats such as MS Word, MS Excel, .jpeg, or .mpeg, to be uploaded and included as assessment evidence.

When selecting a location to store digital assessment evidence, centres must consider the ownership of the materials. For example, if data is stored in a system which is not in the direct control of your centre, eg social media, there is a risk that the evidence may be lost, corrupted or hacked. For security reasons, use of USB flash drives and external hard drives should be avoided where possible.

Training and support

Principle 6: Clear guidance and support should be available for learners, assessors and verifiers on the use of the system(s) including directory structures and naming conventions.

Centres should maintain a digital record with consistent details for each of the systems in use. This could take the form of instructional videos, handbooks or leaflets which can be readily accessed.

Centres should also have a named point of contact for any technical issues arising from use of the system(s).

Centres should consider putting guidance in place on the authentication of content such as video, audio or photographic evidence, to ensure that assessors and verifiers can be satisfied that the evidence has been produced by the learner. This is also covered on pages 8 and 9 of our [Guide to Visiting HN and VQ Verification](#). This guidance will address the question of authentication as outlined in Principle 3 above, while ensuring that the identity of the candidate is protected.

Verification

Principle 7: Wherever possible, digital evidence should be reviewed for assessment and quality assurance in its original location in the system. It should not be sent electronically by e-mail or by any other means.

Where centres have controlled access arrangements in place, these should be used as the preferred option for allowing the review of evidence for assessment and quality assurance. There should be no need for data to be exported from the secure storage.

If possible, there should be the facility to allow external verification to take place remotely and securely. Remote verification provides more flexibility to verifiers and centres. It is done by means of user-access controls, where systems administrators in centres provide verifiers with a username and password that will enable them to login and view the assessment evidence and other assessment materials for a fixed period of time.

Ideally, materials relating to the internal verification process should also be held digitally and shared electronically at the source — or by providing the verifier with remote access to the required, secure location. It is the centre's responsibility to ensure that the verifier's access is removed once verification activity has been completed. For audit purposes, a record should be kept of when this access is granted and removed.

Principle 8: Evidence which is created digitally should remain in digital format throughout the assessment and quality assurance processes.

In most cases, there should be no need for materials to be printed out and scrutinised in hard copy and in some cases, eg videos, this will not be possible. However, there will be exceptions which reflect the skill being assessed. For example, if a learner is being assessed on the skills required to produce a high-resolution graphic, it would be more appropriate and accurate to judge the quality of a printed image. It is the responsibility of the external verifier to make clear what evidence is required to be reviewed in non-digital formats and to justify the reasons for this.

Principle 9: Assessment evidence must be referenced or mapped to the performance criteria or assessment standards and where they exist, templates should be used.

Verifiers must be able to see the assessment standards to which the evidence relates. For this reason, **clear referencing is essential**.

SQA is collaborating with colleges via the College Development Network to develop templates for use with e-portfolios. In this context, a template is a page or collection of pages within an online learning environment, with a set structure that the learner can copy and make their own. The intention is that, once developed, the templates will allow consistency in the structuring and storing of evidence, the provision of feedback, and the processes of internal and external verification.

Appendix: Checklists

The following checklists will help centres and External Verifiers to prepare for verification activity where the evidence is held digitally.

Verification checklist — centre

Verifier: _____

Centre name: _____ Date of visit: _____

Verification group name: _____ Verification group number: _____

Description		Details
1	Is all evidence for the group available digitally or is some on paper?	
2	Is the evidence referenced to the standards?	
3	Has access for the EV to relevant systems been arranged and tested, including user name and password?	
4	Member of staff available from curriculum area to talk EV through approach taken and ensure clarity over location of evidence to be verified.	
5	Have arrangements been made to provide the EV with the other evidence in addition to assessment evidence that they require to make their verification judgement whether this evidence is held electronically or on paper?	
6	Name and contact details of staff member in the centre who can arrange for access and technical support and provide guidance with navigation through the system.	
7	Has access for the EV been restricted to the evidence required for verification?	
8	Does the EV need to access more than one system to review the evidence? If so, is it possible to consolidate the evidence in one place with one login?	
9	Is your Management Information System capable of holding data about which specific courses/units/students have digital assessment evidence in place?	
After the verification activity: has the EV's user account been suspended/deleted?		

Centre checklist — verifier

Verifier: _____

Centre name: _____ Date of visit: _____

Verification group name: _____ Verification group number: _____

Description		Details
1	Is all evidence for the group to be verified available digitally or is some on paper?	
2	Name and contact details of a member of staff from the curriculum area who will be available to talk you through the approach taken and location of evidence to be verified.	
3	Name and contact details of staff member in the centre who can arrange for systems access and technical support.	
4	Has your access to the relevant system(s) been arranged, including user name and password?	
5	Have arrangements been made to provide you with the other evidence, in addition to assessment evidence, that you require to make your verification judgement, whether this evidence is held electronically or on paper?	