Advice for centres in using technology to support assessment remotely

Publication date: April 2023 (Version 1.2)
Publication code: AB8764

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

www.sqa.org.uk

This document can be produced, on request, in alternative formats, including large type, Braille and numerous community languages. For further details telephone SQA's Customer Contact Centre on 0845 279 1000.

SQA is committed to using plain English. We will try to make our publications as easy and straightforward to understand as we can, and will try to avoid all unnecessary jargon. If there's any language in this document that you feel is hard to understand, or could be improved, please write to Editor, Editorial Team, at the Glasgow address or email: editor@sqa.org.uk.

Contents

Introduction

This introduction gives an outline description of remote invigilation. This is the focus of the guidance, although there is a brief mention of the related topic of remote assessment. The two sections, 'Remote invigilation – points to consider' and 'Deciding on a model of remote invigilation – a suggested approach' both highlight the key features that should be addressed in planning and implementation.

In this new version, we have taken the opportunity to position this broad overview more clearly in relation to other documentation that you will be using. If you are looking to implement a model of remote delivery, you will need to consult more widely, as there may be specific requirements arising from the qualification types or assessment content that you are working with.

Invigilation ensures the confidentiality and security of assessments. It also has a role in authenticating a candidate's work as their own. Generally used for exam-type assessments, it helps to satisfy the broader requirement within SQA's quality assurance principles, namely:

'Assessment evidence must be the candidate's own work, generated under SQA's required conditions' (Systems and Qualification Approval Guide, Revised May 2018, Criterion 4.4).

Traditionally, this has taken the form of an invigilator who is physically present in a room or hall, overseeing the conduct of an examination for one or more candidates.

Remote invigilation is where the invigilator and candidate are not in the same physical location. This hasn't played a significant role in the assessment of candidates for SQA qualifications, largely because of the difficulty of designing models that will fit with the quality assurance requirement mentioned above. The recent emergence of 'online proctoring' software has changed this position and allows for real-time monitoring of a candidate and their environment in ways that would not have been possible previously. This can be in the context of 'live' invigilation or using a 'record and review' facility. Similar results can be achieved with other software that provides video and audio links between the invigilator and the candidate.

In general terms, our stance on remote invigilation is the same as it is for other aspects of the way in which centres work with SQA. If a procedure is set up and documented in a manner that complies with our quality assurance requirements — and you can provide evidence that demonstrates ongoing compliance — it will be acceptable.

However, it is our view that remote invigilation is something that needs to be carefully considered. It creates additional challenges from a quality assurance perspective, particularly where the assessment is taking place in the candidate's chosen environment and not one provided by the centre. With a necessarily constrained view of what is happening in that chosen environment, any proposed model will have to work harder to provide reassurance that the integrity of the assessment is not being undermined. Centres will need to carefully balance the advantages of remote invigilation with the likelihood of additional resources being required to make it work satisfactorily.

Importantly, **candidates with assessment arrangements** must be able to access these in a remote assessment scenario. Centres should consider to what extent the existing assessment

arrangements can be implemented remotely and whether additional or alternative arrangements are required to allow the candidate equal and fair access to the assessment. If it is not possible to provide assessment arrangements remotely, it may not be possible to conduct the assessment remotely. Please see assessment arrangements for further information.

There is no 'one-size fits all' model for remote invigilation, and this guidance highlights only those areas that we think need to be addressed when developing your own model. (We suggest an approach on how to do this later in the document.) Once agreed, it may be helpful to have a statement of your agreed approach, together with additional guidance for invigilators and candidates. This will also help SQA's quality assurance team to understand the model you are using.

Remote assessment is where the online link is between the candidate and an assessor, rather than the candidate and an invigilator. Technically, it will share many of the same features as models used to implement remote invigilation. However, the remote assessor is required to play a more substantial role than the remote invigilator. As well ensuring that the conditions of assessment have been met, the remote assessor will need to be satisfied that they have a sufficient view of the candidate's performance to make the required assessment decision. That will obviously vary depending on the nature of the assessment and, if needed, further guidance on this should be sought from the relevant Qualifications Team in SQA.

Remote invigilation: points to consider

- technology and equipment
- data
- assessment content
- assessment environment
- the role of the remote invigilator
- documentation and records
- review

Technology and equipment

It is important that the technology supporting any model of remote invigilation is effective and — for the most part — unobtrusive. It must enable the centre to fulfil its obligation to uphold the integrity of the assessment process, but it must not become a burden or distraction to the candidate. Where a third-party online proctoring platform is used, it is still your responsibility to ensure that the supplier is providing you with the evidence you need to confirm that the process is working as you require.

Whatever combination of technology and equipment is used, you must thoroughly test it before attempting live delivery. There must also be clear lines of support for all those involved, in the event of a technical failure or other incidents.

Data

You will also need to consider the implications for any additional personal data you collect, use and retain as a result of introducing a remote invigilation model. You should consider undertaking a Data Protection Impact Assessment (DPIA) to identify and minimise any data protection risks. This should include any third-party providers who are involved.

Assessment content

Where **question content** needs to remain secure, the model you use must enable this, and you should instruct candidates and invigilators not to take copies of assessment documents. Desktops should be locked down wherever possible, but invigilators will also need to ensure that candidates do not take photographs. This is especially important where fixed assessments (test forms) are used. Confidential assessment material (for example, from SQA's secure website) should not be distributed to candidates as email attachments.

When collecting **candidate responses**, there should be steps in place to minimise any data loss as a result of a dropped connection. You could achieve this by ensuring regular updates to a central server and/or to a local encrypted file.

Assessment environment

As would be standard practice, you should discuss any accessibility issues with the candidate and consider any additional measures that may need to be put in place. If you are not offering an alternative to remote invigilation, this will need to have been made clear during the candidate's induction. You should also make clear who is responsible for providing any additional equipment or accessibility software.

While we will not consider remote locations in the same way as formal alternative assessment sites, we strongly recommend that you issue a checklist for candidates to complete before undertaking a remotely invigilated assessment. This will ask for basic details such as the availability of a quiet space that can be cleared of prohibited items, and access to equipment and internet connectivity. The checklist should also explain the protocol surrounding the conduct of a remotely invigilated assessment, such as the initial environmental sweep, and how to minimise behaviour that could appear suspicious. You should also consider whether to include a trial run prior to the assessment or to build in additional time on the day to allow for technical checks.

The role of the remote invigilator

Remote invigilators should be given a clear description of the role they are being asked to perform, and should be trained in the technical set-up. This will help to settle the candidate and allow them to focus solely on the assessment.

Equally important, the invigilator should have the skills and confidence to enforce the conditions required to prepare and maintain a remotely invigilated environment. This will include an agreed method for authenticating the identity of the candidate and an initial sweep of the immediate surroundings to ensure that they comply with the guidance issued previously to the candidate. It will also include giving directions to the candidate if anything unusual is detected in the course of the assessment. There should be an agreed escalation of warnings up to, and including, abandonment of the assessment session.

Invigilators will need to ensure that they have a sufficient perspective to fulfil their function. For example, if there is no desktop feed or lockdown, how can they be sure that they are able to monitor both the desktop and the candidate? Could the candidate be accessing other applications, using messaging services or receiving assistance? What happens if there is an interruption to the audio-video connection?

Once these details have been agreed, you should review and confirm that your safeguarding policy is adequate to cover this role.

Documentation and records

As suggested, a single statement of your approach to remote invigilation would be helpful. This can be standalone, or could be incorporated as amendments to existing policies and procedures within your centre.

We may expect the following core documents for all remotely invigilated assessments:

- a detailed description of the role and responsibilities of the remote invigilator
- formal guidance and technical help notes on the technology being used to support remote invigilation
- a concise guide for the candidate — information on how to select and prepare their assessment environment and how to minimise any behaviours that may appear suspicious during the assessment

We would expect the following records for all remotely invigilated assessments:

- completed and returned candidate checklists
- completed invigilator reports

Invigilator reports should note any technical interruptions and any irregular behaviour identified during the assessment session. If an investigation of potential malpractice is required, it should follow your standard procedure.

Records should be retained and disposed of in line with your local retention schedule and SQA's quality assurance requirements.

Review

You should periodically review the operation of your model for remote invigilation, particularly in the initial stages. This should involve feedback from the invigilators and candidates. It should also look at the checklist given to candidates to ensure that it is clear and sufficient in what it is asking of them in terms of preparation for, and conduct during, the assessment.

It should also include a review of results, looking for any unusual or unexpected patterns, for example:

- Are any identifiable individuals or groups of candidates doing better or worse than expected?
- Does this in any way correlate with the feedback you have received from candidates or invigilators?

This will give you a chance to improve the support and documentation given to invigilators and candidates.

Deciding on a model of remote invigilation — a suggested approach

In this section, we will consider the key points you will need to address when developing your own model of remote invigilation.

Balancing risk and practicability

In everything that follows, you should be thinking about any increase in threats to the integrity of the assessment as a result of moving to a remote invigilation model. For example:

- Are you concerned about a reduced ability to confirm that the candidate is who they say they are — the problem of *personation*?
- Are you concerned that assessment material you are required to manage as confidential will be copied and find its way into the public domain?
- Are you concerned that your ability to uphold the required assessment conditions (such as closed book or no collaboration) will be constrained?

If so, you will want to find solutions that address these concerns and reduce the risk that the assessment will be compromised. These solutions need to be *practicable* — in terms of the technology being used, the knowledge and skills of those using it, and the extent to which the model is scalable as volumes increase. Even when you are sufficiently confident to proceed, you should periodically review the model in operation, to confirm that the balance is working effectively.

How will you ensure the continued security and integrity of assessment content?

SQA quality assurance criterion 4.5 requires assessment materials to be stored and transported securely. It goes on to note ‘In particular, this relates to assessments where a candidate would gain an unfair advantage by seeing the assessment in advance and the assessment is carried out under controlled conditions.’

Consider:

- How can you ensure that the candidate does not see the assessment until the point at which the assessment session begins, and the appropriate assessment conditions are in place?
- When delivering remotely, you cannot gather in paper copies as you would at the end of a traditional invigilated assessment. Given that, how can you ensure that the candidate is not able to copy all or parts of the assessment and pass on to others? That could be directly from the screen or as an image taken using a mobile phone.

Examples:

- Use software that allows access to the assessment content only once the assessment session has begun. Ideally this should be linked to a timer that automatically limits the duration of the session; at the very least there should be an audit trail of timings.
- Using software that can lock down the desktop (SOLAR’s SecureClient, a secure browser or similar). This puts the device in ‘kiosk’ mode — blocking access to other applications while the assessment is running.
- Use a camera set-up that gives the remote invigilator a full and continuous view of the candidate’s screen and immediate working environment.

How will you accurately authenticate candidates?

Consider:

- This is not usually a major issue where candidates are well known to the centre and physical matriculation or similar identity cards can be used for traditional invigilated assessments — but it can be more challenging to implement online.
- The assessment should not proceed unless all reasonable steps have been taken to confirm the identity of the person at the end of the online connection.

Examples:

- Requiring the same identity evidence as you would at the centre — use video link to check possession of identity card and then confirm with a clear view of the candidate's face.
- Including time for authentication as part of the assessment — part of the 'settling in' procedure.
- Facial recognition software is also promoted for this purpose. Again, a balance needs to be struck between the additional benefit this may provide and the data privacy issues it raises.

How will you uphold assessment conditions, including invigilation requirements?

Consider:

- How can you ensure that you meet the same standard of invigilation as you would if the assessments were being conducted in a centre? This means that candidates should not be able to access prohibited materials (physical or online) or collaborate with third parties (physically present or online).

Examples:

- Using a desktop lockdown or secure browser will close off other communication through the device delivering the assessment. A single camera view on the candidate and their immediate environment can then check that other devices and resources are not being accessed.
- In the absence of this, you should be looking for a camera set-up that allows invigilators to clearly see the screen or device, the candidate, and the immediate environment. Depending on the circumstances this may require one or two cameras.
- Clear guidance materials to help your remote invigilators to carry out their role confidently and effectively.

How will you ensure equity of assessment?

Consider:

- How will candidates have the practical and technical requirements to be able to access the assessment?
- How will adjustments be made for any accessibility requirements?
- How will you ensure that the location of the assessment will not negatively impact on candidate outcomes?

Examples:

- Technical requirements are made clear to candidates.

- A technical check is carried out in advance of the assessment and sufficient time is left for changes to be made.
- Candidates are to be made aware of invigilation requirements and how the assessment will be carried out.

How will you review the effectiveness of these arrangements?

Consider:

- Are candidates and invigilators comfortable with the roles they are being asked to perform in the process?
- Is the method of delivery having any impact on your assessment outcomes (positively or negatively) — and are you comfortable with this?

Examples:

- Short surveys or other feedback from candidates and invigilators.
- Periodic reviews as part of regular internal verification or other quality assurance arrangements.