Advice for centres in using technology to support assessment remotely

December 2020

The information in this document may be reproduced in support of SQA qualifications only on a non-commercial basis. If it is reproduced, SQA must be clearly acknowledged as the source. If it is to be reproduced for any other purpose, written permission must be obtained from permissions@sqa.org.uk.

© Scottish Qualifications Authority 2020

Contents

Introduction

Overview

The **Introduction** gives a brief outline of remote invigilation. **Remote invigilation – points to consider** and **Deciding on a model of remote invigilation – a suggested approach** both outline the commonly understood approach to remote invigilation. However, we recognise that 2020-21 poses additional challenges that may mean that the ideal approach is not attainable. For specific guidance on 2020-21 please refer to the last section in this document – **Remote invigilation 2020–21 — temporary adjustments**.

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, this may not be a suitable arrangement. Please see assessment arrangements for further information.

Invigilation ensures the confidentiality 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'[1].

Traditionally, it 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. Although the approach isn't new, it hasn't played a significant role in the assessment of candidates for certification of SQA qualifications. This is partly because of the difficulty of designing models that will fit with SQA's quality assurance requirements mentioned above.

The emergence of 'online proctoring' and similar software has changed this position to some extent, allowing for real-time monitoring of a candidate and their environment in a way that would not have been possible previously. And now, with COVID-19, we have a situation where the traditional set-up for invigilation may be very difficult or practically impossible to arrange.

The first thing to make clear is that there is **no blanket prohibition on the use of remote invigilation** in SQA's policy statements or guidance on the delivery of assessment. There may be assessments and qualifications for which this method of delivery is judged not to be appropriate, and we will aim to state this explicitly in these cases. However, in general terms, the position 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 SQA's quality

[1] Systems and Qualification Approval Guide, Revised May 2018, criterion 4.4.

assurance requirements — and can provide evidence that clearly demonstrates ongoing compliance — then it will be acceptable.

However, it is our view that remote invigilation is something centres need to think about carefully before proceeding, as remote invigilation creates additional challenges from a quality assurance perspective, particularly because 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 they anticipate arising from the introduction of remote invigilation with the likelihood of additional resources being required to make it work satisfactorily.

We cannot offer a 'one-size fits all' model for remote invigilation. This guidance highlights only those areas of the quality assurance criteria that we think need to be addressed when developing your own model. A suggested approach on how to do this is given 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 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. It must not become a burden or distraction to the candidate.

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.

Data

You will also need to consider the implications for the 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 that may be created by the use of remote invigilation.

Assessment content

Where assessment content has to remain secure, the model you use must enable this, and you should instruct candidates and invigilators not to take copies. Desktop lockdown should be enabled wherever possible, but invigilators will also need to ensure that candidates do not take photographs. This is especially important where fixed assessment versions are used, although you should also take care with item bank rules-based objective tests. If possible, you should not send secure assessment content (for example from SQA's secure website) as email attachments to candidates, as that can increase risk of its exposure.

You should also attempt to take steps to minimise any data loss from a candidate's response during the assessment when online or remote. You could achieve this by 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, then this will need to have been made clear at candidate 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 do recommend that you issue a checklist for candidates to complete prior to 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 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 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.

Depending on the set-up, invigilators will need to ensure that they have a good enough perspective to fulfil their function. For example, if there is no desktop feed or lockdown, can they be sure that they are able to monitor both the desktop and the candidate? Could the candidate be accessing other applications, messaging services or be receiving assistance?

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. But it may — and eventually probably will — 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 have attached follow-up notes if any suspicious behaviour has been identified during the assessment session. This should include a review of any evidence, a statement from the candidate, and an audio-video recording (where this exists). Decisions taken on the basis of this review should be made clear.

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, at least 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 documentation and support given to invigilators and candidates.

Deciding on a model of remote invigilation — a suggested approach

As the preceding guidance has explained, the position of SQA is that remote invigilation of assessment is an option centres can use. We don't require the use of any specific method or technology. There are too many options to do so and a 'one-size fits all' approach would not be appropriate for all centre types and all qualifications. What we require is that any set-up chosen — and, importantly, the way that it is administered — can be shown to comply with SQA's quality assurance criteria.

As the guidance has indicated, this will require some planning and preparation from centres thinking about using remote invigilation. In this section, we aim to structure that process and address all the key points that underpin good assessment delivery. This may lead you to a model that works for you and your candidates — but it may not, and it is important to recognise that this mode of delivery may not be appropriate or workable in all circumstances.

It is important to stress that this is our general approach, and it may be that the assessment arrangements for specific qualifications override this. That may include the requirement to use a specific piece of software; it may even preclude remote delivery entirely.

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 also 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, secure browser or similar). This puts the device in 'kiosk' mode — blocking access to other applications (such as screen grab) while the assessment is running. Mainly for desktops and laptops — this will be more challenging for personal devices such as tablets and mobile phones.
- 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 clear view of candidate's face.
- Online tools that use facial recognition software — useful for high-stakes assessment where candidates are not well known to the centre.
- Including time for authentication as part of the assessment — part of the 'settling in' procedure.

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.

Remote invigilation 2020–21 — temporary adjustments

Due to the unprecedented circumstances in which we find ourselves, we recognise that some temporary adjustments to assessment practices may be required for the academic year 2020–21.

Open book assessments

For the duration of the academic year 2020–-21, for certain qualifications you are able to carry out assessments under more flexible open book conditions. There are however some qualifications that due to their high-stake nature, or particular regulatory requirements, must not be undertaken in this way.

Consider:

- What resources would be useful to candidates as part of the assessment?
- How will you ensure that candidates are not receiving help from other sources, for example another person?
- How will you ensure that the responses are the candidate's own work?

Examples:

- In addition to relevant books or resources, you may also wish to allow access to software tools such as calculators, spellcheckers or internet-based resources.
- Make clear to candidates ahead of time what they should and should not access for the duration of the assessment.
- By upholding the assessment conditions (as listed above) you will be able to see if the candidate is receiving help from other sources.
- The time-limited nature of the assessment may have an impact on the amount of research that a candidate may reasonably be able to do. Consider how you make this clear to candidates so that they can manage the assessment time effectively.
- Candidates may be asked to complete a declaration to confirm that they have adhered to the conditions of assessment.

Use of cameras for invigilation purposes

We understand that in some circumstances the use of cameras may be prohibited. If there is no possible way to use cameras for invigilation or indeed no other means of carrying out the assessment (for example delaying the assessment until it can be administered in person), then you can try and limit the time that the assessment is available to the candidate before it is submitted. You can remind them of the conditions of assessment and ask for a confirmation from the candidate and (perhaps) another witness, that these have been adhered to. Centres should consider whether this mode of delivery has had an impact on assessment outcomes and whether supplementary evidence should be sought.