# OAL Remote Assessment Platform

During the current Covid-19 Crisis, OAL has been quick to respond and ensure that assessments could continue remotely, where the Assessment Plan allows.

In order to make this move to remote assessment we had to identify a platform that would meet the stringent needs of the various Quality Assurance Organisations that inspect us, as well as having a user friendly interface that would meet the requirements of assessment and allow ease of access for apprentices and assessors.

We reviewed various platforms, including Skype, MS Teams and Google Hangouts and made the decision that Zoom was the best option and subsequently got approval from our various EQA bodies and the Institute for Apprenticeships to use it for remote EPA.

The reasons Zoom was selected included the following:

- Screen Sharing facilities – both the assessor and the apprentice can easily share a screen at the touch of a button
- The ability to cede control of a laptop/computer from the assessor to the apprentice – This helps maintain the security and integrity of the test as the test never needs to leave the assessor's computer
- Reliability – we found zoom the most reliable of all the systems, with the easiest access and little interference.
- Quality, both the audio and visual quality of Zoom out performed other platforms
- We need to be consistent in our approach and systems with the Quality Assurance bodies
- OAL must ensure that one platform is utilised to prevent over exposure of numerous systems and to also confirm that our Independent Assessors are trained in detail on one system.

We are aware of some concerns over the Zoom security functionality, however the platform has now addressed all of these issues and reports of security breaches are now out dated.

We would like to reassure our Customers, that we have invested in purchasing licences with Zoom as our preferred platform and confirm security functions that are now in place with Zoom as highlighted below.

## 1. Secure Networking

Good news! All Zoom meetings are also protected by multiple security layers with flexible controls.

- Cloud Infrastructure: Zoom meetings run on our highly reliable, scalable, secure infrastructure platform in the cloud. A distributed network of low-latency multimedia routers resides on Zoom's communications infrastructure. All session data originating from the host's device and arriving at the participants' devices is dynamically switched — never stored persistently.
- Encryption: Zoom secures session content by encrypting the web communications channel to https://zoom.us. Zoom also supports SSL/TLS (port 443) network-layer communications between the Zoom app and the multimedia router, as well as NIST AES 256 application-layer encryption.

- Post-Meeting Security: Once the meeting is over, no session information is retained on the Zoom routers or on any participant's devices. If a meeting is recorded, the recording is located on that customer's local machine or in the secure Zoom cloud if selected.

## 2. Scheduling Features

Here are some features you can access when you're scheduling your meeting to make it more secure:

- Password Protection: Password protect your meetings by clicking Require meeting password and entering an alphanumeric password when you schedule your meeting. The password is automatically populated in the calendar invitation. This means that only people with both the meeting ID and password can join your meeting.
- Join Before Host Options: When scheduling, you have the option to either allow participants to Join Before Host, or not. If you don't select this option, no one can join the meeting without you being there to start the meeting. This gives you greater control over the meeting. Even if you do select Join Before Host, you still get an email notification when they join before you.

## 3. In-Meeting Features

The meeting host has a variety of controls they can use to secure their meeting. For example:

- Lock the Meeting: When you're in the meeting, click Participants at the bottom of your Zoom window. In the participants' pop-up box, you will see a button that says Lock Meeting. When you lock the meeting, no new participants can join, even if they have the meeting ID and password.
- Expel a Participant: In the participants' menu, you can mouse over a participant's name, and several options will appear, including Remove. Click that to kick a participant out of the meeting. They can't get back in if you then click Lock Meeting.
- Waiting Room: Protect participant privacy by keeping some participants in your virtual waiting room while you finish up meeting with others.
- Attendee On-Hold: If you need a private moment, you can put attendees on-hold. The attendee's video and audio connections will be disabled momentarily. Click on the attendee's video thumbnail and select Start Attendee On-Hold to activate this feature.

Other host controls include locking screen-sharing, enabling/disabling participant recording, watermarking screen shots, and disabling in-meeting chat.

## 4. Advanced Security Options

Some enterprises have additional security needs for video and web conferencing. Zoom at your service!

- Meeting Connector: The Zoom Meeting Connector is a hybrid cloud deployment method which allows a customer to deploy Zoom within the company's internal network. The meeting administration is managed on Zoom's infrastructure, but the meeting itself is hosted in the company's internal network. All the meeting traffic, including audio, video, and content sharing stays within the company's own network. This leverages your existing network security setup to further protect your communications.
- Single Sign-On (SSO): With SSO, a user logs-in using your company's identity provider such as Microsoft Active Directory, Centrify, Okta, or Google to access a variety of applications. Zoom works with all SSO providers via SAML or OAuth so you can easily assign who gets access to Zoom. Zoom also offers an API call to pre-provision users from any database backend. With Zoom, you can map attributes to provision a user to different groups with feature controls.

OAL has adopted all of the recommended security features and apply these to all remote assessments.

This insures that our assessments and your systems remain safe and uncompromised.