How To Improve The Security Of Your Online Meetings: A Guide For Open Arms Staff

The following guidance has been developed to assist all Open Arms staff in considering and implementing the necessary actions to reduce the risk of sensitive information being accessed when using online platforms.

Checklist:	
1. Ensure naming conventions of invitations / topics / chat or meeting room names do not contain identifying information or classified information in the title.	☐
2. Avoid distribution of meeting passwords beyond the intended participants.	☐
3. In the online meeting settings, confirm (where applicable): "*Require meeting password*" is enabled. "*Recording of session*" is disabled. *For additional information on where these settings can be found, refer to the help setting at each video platform website.*	☐ ☐
4. Consider the use of the virtual 'waiting room' function. This allows the host to admit only known parties in to the session.	☐
5. All parties should consider the use of earphones or a headset, and ensure that devices are only transmitting audio to a single output (i.e., headset, computer speakers, and earphones). This will ensure audio is only being heard by the intended recipients.	☐
6. Consider your working environment; do you have privacy and an uninterrupted space for the duration of your meeting?	☐
7. If applicable, ensure all your client service delivery documents relevant to the meeting are stored in a secure manner.	☐
8. Ensure any confidential documents are locked away in a secure place.	☐
9. Ensure the device(s) being used (by all participants) has up-to-date software, including Operating System, Anti-virus and online video platform software.	☐

It is important that this guidance is considered for both client-facing and colleague-facing virtual interactions, as both may be associated with risk concerning sensitive information.

For further guidance, please refer to DVA's Records Management, Security and Privacy policy, located in the Guidelines for Working from Home section on the DVA Intranet or use this link.