

|  |
| --- |
| Guidance for using and choosing video conferencing apps |
| What to consider before you decide on a video conferencing app  |

Contents

[Introduction 1](#_Toc42156053)

[How to ensure your video conferencing meetings are secure and private 1](#_Toc42156054)

[Further information: 2](#_Toc42156055)

# Introduction

Working from home has become the new normal for most people. To support this new way of working, many people have turned to video conferencing applications to have online meetings and collaborate. Video conferencing applications are great tools to facilitate and support remote working, but not all video conferencing tools are equal when it comes to ensuring the privacy and security of your meetings and their use can introduce security and privacy risks into your organisation. You cannot always “see” the meeting participants nor can you be sure of who is listening in, so you are dependent on the security features that your video conferencing application provides to ensure the privacy of your meetings.

DHHS recommends, and uses, Microsoft Teams and Cisco’s Webex for video conferencing. Microsoft Teams is part of the Office 365 suite of applications and Webex allows participants to join via a browser rather than a direct installation of the application. DHHS recognises that not all organisations have moved to Office 365. These guidelines are written to provide you with confidence that no matter which video conferencing application you use, you can take steps to ensure that your meetings are secure and private.

## How to ensure your video conferencing meetings are secure and private

### Configure the application for security

Check that the default security configurations meet your organisation’s security requirements. If you are unsure of your organisation’s security requirements, check with your IT support team. Settings or features that will increase the security of your meetings include:

* ability to control and monitor how and who can record the meeting.
* notifications to alert the organiser when a person has joined a meeting.
* functionality that allows you to blur or hide your background.

If you are using video conferencing from your own device, make sure that your device has the latest operating system and security updates.

### Plan your meeting discussions in advance

Consider whether the information and topics to be discussed are appropriate for video conferencing.

Be aware of any records management and compliance requirements for your meeting. For example, which part of a meeting becomes a 'record', e.g. time/date/agenda/files shared/chats etc. so that these can be retained.

Apply a risk management approach when deciding which topics and/or discussions that would pose a risk of harm if exposed or compromised.

### Establish meetings securely

When organising a video conferencing meeting, make sure that you send the invitations to only those people who should attend. Also ensure that the details and link to your meeting are not publicly available. Use the settings to control who can be present in the meeting and who should wait in the “lobby” before joining.

### Be aware of unidentified participants

Confirm that all meeting attendees are who they say they are. You may wish to ask people to go around and introduce themselves or say, “Hi”.

Ask attendees to advise the meeting organiser if someone else will be attending the meeting on their behalf before the meeting starts and to provide their details.

### Be aware of your surroundings

A private location when participating in meetings ensures that your discussions won’t be overheard. If it’s difficult to find somewhere private, try using headphones so that only half the conversation may be overheard.

If you turn on your camera when meeting, make sure no sensitive or confidential information is visible to participants. You may also use the option of changing or blurring your background if this feature is available on your video conferencing application.

### Be mindful of your conversations

During work meetings, sensitive and private topics are often discussed. Try to keep discussions to the agreed topics.

### Only share what is required for the meeting

Only information that is relevant to the meeting topic discussions should be made available to participants. If the information has protective markings or a security classification, indicate this before sharing so that participants are aware of the expectations in handling that information. If you need to share content on screen, it is best practice to use the individual application(s) e.g. MS Excel for spreadsheet, rather than your whole device screen.

## Further information:

### Handling and using protectively marked information and data

DHHS is implementing protective marking on all its information resources. By using these protective markings, the information’s sensitivity level is flagged to the recipients and users. These act as a guide on how to handle, share and store the information based on the protective marking of the information.

You can find more information about assessing the security value of information at: <https://ovic.vic.gov.au/resource/practitioner-guide-assessing-the-security-value-of-information-v2-0/>

### Selecting a secure Video conferencing application[[1]](#footnote-2)

You may not be the person responsible for selecting the video conferencing application for your organisation. For those who are tasked with choosing a video conferencing application for your organisation, the following questions may be useful in guiding your choices.

#### What is the difference between a paid and free video conferencing application?

A paid service will usually include a commercial contract and more stringent terms and conditions of use as well as better privacy and security controls compared to a free service.

Be aware that with a free video conferencing application, you are not buying a product to consume. The data and information that you generate when you use a free video conferencing application is available to use or sell for profit by the provider of the video conferencing tool.

It is always recommended to use a paid service for video conferencing for work use.

#### Where is the location of the video conferencing provider?

Sometimes the application provider is based in a country outside of Australia. Their privacy and security protection laws may be different to ours; the provider may lawfully access your ‘secure’ data without your approval.

#### Does the provider take security and privacy seriously?

Choose a provider that is responsive to cyber security or privacy issues when they arise and who engages with their customers’ privacy and security advocates.

Do some research on the providers’ past responses to security and privacy issues raised in relation with their application.

#### Do the app providers’ terms and conditions address legal, privacy and security requirements?

The terms and conditions should set out specific clauses around legal, privacy and security requirements. Without these requirements being specified, your organisation will not be able to verify the application provider’s security claims and confirm that your information is being used as expected. The terms and conditions should clearly state what claims the application provider has to the data that is created from the meetings, such as voice data from the meetings, meta data about the meeting or files that are created or shared during the meetings.

#### What **information about your meetings does the video conferencing provider collect and store?**

Information such as, but is not limited to, names, roles, organisations, email addresses, and usernames and passwords of registered users, as well as information about devices used are typically collected and stored by the provider.

Your organisation should provide advice to staff as to the appropriate sensitivity level of information they should disclose during a video conference session.

Knowing how your meeting information is captured and stored by the provider will inform the legal, security and privacy risks your organisation has when using the video conferencing application.

You are also trusting the web platform provider to respect the privacy of the metadata i.e. who-met-when-to-discuss-what, and to not record or share the audio/video/documents shared in the meeting without your authorisation.

#### Does the video conferencing provider use strong encryption?

Information stored with the provider (at rest) and when it is being transferred via different devices (in transit) should be encrypted to ensure it is secure from unauthorised access.

When considering a video conferencing provider, check that they use Transport Layer Security (TLS) which is a strong encryption protocol that protects data in transit. Note that web conferencing solutions that exclusively support TLS versions 1.2 and 1.3 inherently offer more protection for data transmitted across untrusted networks such as the internet. Know that you are trusting and relying on the video conferencing provider to maintain a high security environment so that they are not hacked by criminals and prevent from their data being stolen.

#### How reliable and scalable is the video conference application?

The video conferencing application should have the capability to grow with demand while continuing to provide a reliable and secure service. Understanding the capabilities of the video conferencing application such as the number of simultaneous connections that can be supported will enable staff to meet and collaborate even during times when demand for video conferencing is high. If your current video conferencing application cannot meet demand, then consider either increasing the capacity of the existing video conferencing application or looking at other means of information sharing. Before moving to an alternative solution, be aware that any alternate solution would need to be reassessed to ensure that no security, privacy or legal risks are introduced.

|  |
| --- |
| To receive this publication in an accessible format email the Cyber Security Management team, info.security@dhhs.vic.gov.au .Authorised and published by the Victorian Government, 1 Treasury Place, Melbourne.© State of Victoria, Australia, Department of Health and Human Services April 2020. |

1. This section uses information from Australian Cyber Security Centre (ACSC), <https://www.cyber.gov.au/publications/web-conferencing-security>, guidelines [↑](#footnote-ref-2)