Government of Newfoundland and Labrador
Department of Justice and Public Safety
ATIPP Office

Guidance on Conferencing Software

The ATIPP Office provides the following information in response to questions received from public bodies about using video conferencing software to conduct meetings, both public and private, during the Covid-19 pandemic.

For public bodies which are served by the provincial government's Office of the Chief Information Officer (OCIO), Skype for Business is recommended. OCIO can provide assistance if Skype for Business is not meeting your needs. For other public bodies, there are a number of options available (e.g. Skype, Zoom, WebEx, Google Meet, Facebook Messenger, etc.).

There are privacy and security risks associated with all information sharing software. For example, recently there have been numerous reports of unauthorized individuals hijacking online meetings and displaying hateful or pornographic material. It appears that in many cases unauthorized individuals gain access to the meeting because the meeting link is available publicly. If you are hosting meetings, you should be aware of these risks and how to mitigate them. Each organization must do its own due-diligence as is reasonable in the circumstances.

If you intend to use video conferencing software, we make the following recommendations:

1. If possible, seek advice from IT professionals prior to employing new technology.

2. Review the software company's privacy policy and encourage other users to do the same. Depending on what the privacy policy is, you may determine that the technology is appropriate to use in most circumstances, but not adequate for certain meetings where confidential or sensitive personal information is being discussed, collected, etc. The privacy policy should be easy to locate on the company's website.

3. Participants in meetings should be provided a privacy statement prior to meetings. If personal information is being shared during the meeting (which could include information shared when participants join meetings from cell phones or home computers) ensure that all participants are aware that there may be some collection of personal information, and highlight any privacy concerns particular to the software you are using. The ATIPP Office is happy to assist you with drafting a privacy notice.

4. Inform participants whether or not a meeting will be recorded. If a meeting is recorded, the recording must be an authorized collection under the **Access to Information and Protection of Privacy Act**, (**ATIPPA, 2015)** and used, disclosed, and disposed of in a manner consistent with **ATIPPA, 2015** and other relevant legislation and policies.

5. Familiarize yourself with the privacy and security settings of the software and test the software prior to the meeting. For example, particular settings may allow you to password protect a meeting so that only invited participants are able to attend. You may also be able to adjust settings so only the person hosting the meeting can share content.

6. If a meeting involves a large number of participants or is a public meeting, you may wish to ask participants to register with an email. That way, you can share a meeting link or meeting password privately.

7. During the meeting, designate another individual to monitor the meeting for irregularities, and obtain the identity of those joining the meeting.

8. Where a meeting is open to the public, or the audience will be large, it may be more secure to broadcast a live stream to the audience in a manner which does not provide them with the ability to participate, and does not share their personal information. In other words, they should be an audience as opposed to participants.