MCFD MS-Teams Security and Privacy Guidelines

These guidelines are for the use of MS-Teams in relation to MCFD programs subject to *Freedom of Information and Protection of Privacy Act* (**FOIPPA**) or *Child, Family and Community Services Act* (**CFCSA**).

Cloud-based applications are only as secure as, the settings you put in place and your compliance with security, privacy, and records management policy and guidelines. Privacy incidents or privacy breaches that severely impact ministry clients, the ministry and government itself can occur when these guidelines aren't followed. Staff members should exercise caution and good judgement on whether MS-Teams is an appropriate tool to use, based on the sensitivity of the information involved.

- **MS-Teams is not to be used for *Youth Justice programs and services* as it has not yet received security and privacy approval.**
- Staff within Delegated Aboriginal Agencies (DAAs) must follow these guidelines when undertaking CFCSA work.
- Third party service providers using MS-Teams must follow these guidelines. Service providers do not need any license to participate in ministry-initiated Meetings/Chat; However, service providers who purchased their own Microsoft Office 365 license and if federated by the OCIO can also initiate meetings/Chat with ministry staff.
- Child Protection Mediators are unable to access government's enterprise licence for MS Teams. Mediators can purchase their own Microsoft Office 365 license or MCFD staff can initiate the Meetings while adding both mediators and clients as "guests" (MCFD staff do not have any options within MS-Teams to delegate "organizer" roles to guests).

General Advice

1. Meetings, Teams, Chats and File-sharing can be used for subjects involving **non-personal** or **non-confidential** information and does not involve clients.
2. Only Meetings functionality can be used when **client, personal or confidential information** is involved.
3. Do not share documents containing client, personal or confidential information using the File Share function. Instead allow others to view the document using a shared window. Make sure you are sharing the relevant window not the entire desktop.
4. Be aware that Chats are persistent and retained in MS Teams. If you accidentally type sensitive information in the Chat window, you can only delete it from the Chat view. While users can "delete" information so it is not visible to themselves or other participants, the information continues to be stored in the background and is subject to Freedom of Information (FOI) requests.
5. MS-Teams is not an appropriate recordkeeping system for government records. Employees are responsible for ensuring relevant business information that is created or received is summarized, transcribed or copied to another document and stored in the appropriate ministry recordkeeping system.

6. You can use MS Teams apps (MS Planner, OneNote, Stream, etc.) for transitory and non-sensitive information. For all other cases, contact your Ministry Privacy Team.

Attending or Hosting a Meeting

7. Do not include client names in the subject line in your Meeting invite as everyone with access to your calendar can see this information. If the Meeting is about an HR issue, do not include staff names in the Meeting subject line.
8. Email addresses and/or phone numbers of invitees are visible to all other participants in the Meeting. This is an issue in situations where clients do not want their contact information disclosed to other Meeting attendees. If this is the case, do not use MS-Teams for those Meetings.
9. Be aware when the camera or microphone is on. Best practice is to turn off or mute when not engaging.
10. Choose a physically private location when using audio or video conferencing to prevent eavesdropping and disclosing personal information about yourself, others in your home or workplace, and about the clients we serve (e.g. pictures of family on the wall, etc.). Guests should be reminded of this as well. Use MS-Teams background images or simply select "turn on video to use blur" option before joining the Meeting.
11. For Meeting organizers, designate yourself as host or sole presenter with guests but adjust according to the needs of the Meeting. The options selected during the Meeting creation time, are permanent; once Meeting created, host or guest wouldn't be able to change any options.
12. Restrict all guests (outside of government network) from bypassing the lobby.
13. Beware that guests can easily spoof their names as someone else. Organizers do not have any options to verify the identity of the guest before they join the Meeting. As of now, there is NO known remedy for this issue.
14. A Meeting host may ask others not to record the Meeting. Be aware that any participant could begin recording at any time using another device. Always be professional.
15. During a Meeting with "guests" the organizer/host must make sure to click "**end Meeting**" option before leaving the Meeting.
16. Ministry staff participating in MS-Teams meetings hosted by other parties may disclose client, personal or other third-party information only if all parties have the authority to collect or use the information.

Recording, Translation or Live Captioning in Meetings

For programs under the CFCSA, recording, live caption, or translation functions must not be used as it does not comply with legislation. *(For non-CFCSA programs recording, live captioning and translation is permitted by* Ministerial Order-M180 *only until Dec 31st, 2020. After this date these functions will no longer be compliant with legislation.)*

17. Do not record meetings unless necessary for valid business reasons.
    - We are authorized to collect only the information that is considered necessary for program purposes, often, more information is captured than necessary when recording. Advise all participants before the recording starts.
18. Be aware that setting recorded video permissions to "Allow everyone in your company to view this video" will make the video accessible to all of BC government employees.
    - If you retain the default settings, only Meeting attendees will have access to the recording.
19. Summarize and save the pertinent information or transcription from your MS-Teams Meeting or Chat within your regular recordkeeping systems (LAN, ICM, CRIS, physical files). Refer to the MS-Teams Record Management Guide for more information. Promptly delete the recording as this is now transitory information. You can delete your recordings by signing into this portal https://web.microsoftstream.com/browse.

MS-Teams Support Model

MS Teams Ministry-Specific Support	Social.Sector.Service.Desk@gov.bc.ca
Technical Questions	• First-level Support call 7-7000 (250-387-7000) – Option 1 or • Online support 24x7: OCIO My Service Centre
Privacy Questions	MCF.PrivacyImpactAssessment@gov.bc.ca
Security Questions	SDSIINSEC@gov.bc.ca