U.S. Department of Health and Human Services
Administration for Children and Families
Office of Family Assistance

National Responsible Fatherhood Clearinghouse

FATHERS INCORPORATED

INTERNET SECURITY:

Ensuring Confidentiality and Privacy When Using Virtual Technology[1]

NRFC TIPSHEET

This National Responsible Fatherhood Clearinghouse (NRFC) Tip Sheet is a Companion Document to the NRFC Spotlight *Using Virtual Technology In Fatherhood Programs.*

LINK TO SPOTLIGHT WILL BE ADDED WHEN THE SPOTLIGHT IS POSTED TO NRFC WEBSITE

SELECTING A VIRTUAL PLATFORM

- If possible, use a web conferencing platform that is FedRAMP[2] certified.
  - See *https://marketplace.fedramp.gov/#!/* products for a list of FedRAMP authorized cloud-service products.
  - Any organization that purchases a subscription or license to the service can use these products. However, the versions of the products in this list are designed to be used by government agencies.
- Ensure that all staff are trained in the privacy and security functions of the platform(s) you select.

LIMIT ATTENDANCE TO INVITEES ONLY

- Set up passwords for all meetings.
- Change meeting IDs or codes frequently.
- Do not post information about the meeting on social media, unless necessary.
- Enable the "waiting room" option (if it is available on the platform you are using) to:
  - Ensure that the meeting cannot begin until the host joins.
  - Allow the meeting host to verify all participants before admitting them to the meeting.

[1]Rupinder Randhawa, IT Project Manager, ICF, compiled these tips.

[2]FedRAMP (Federal Risk and Authorization Management Program) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

MANAGING AN ONLINE MEETING

A. Enable notification when attendees join by playing a tone or announcing names.

- If this is not an option, make sure the meeting host asks new attendees to identify themselves.

B. If a dashboard (or similar platform control) is available, use it to monitor and identify all attendees.

C. For web-based video meetings:

- Caution all users who intend to share their screen to be mindful not to inadvertently share other sensitive information during the meeting.
- Allow users the option either to preview video and select a virtual background, or to join without video.

D. Enable and use the following options as needed:

- Put participants on hold
- Remove participants
- Mute participants
- Disable video
- Disable file sharing
- Disable private chat
- Disable annotation
- Control screensharing
- Control recording

FOR EXTRA SECURITY

Require participants to use a personal identification number (PIN) or two-factor authentication to access a meeting.

If part of a meeting will cover sensitive or confidential information restricted to a subgroup of attendees, enable "remove participants" and/or "terminate access" options.

- This ensures that participants not invited to a specific portion of the meeting have indeed left and cannot rejoin until the host permits.

RECORDING ONLINE MEETINGS

A. Obtain consent from all participants before you record a meeting.

B. Make sure meeting recordings are encrypted.

C. Only record the meeting when absolutely necessary.

Disclaimer:

Some virtual meeting platforms may not offer all of the features mentioned in this list of tips. In addition, users may need to update their equipment and/or software to utilize some features.