The Trust

in partnership with the Alliance and SCIP

TELECONFERENCE APPLICATION SECURITY TIPS

The Trust's teleconference security tips appear below. These tips should be considered general guidelines that can be tailored to each district's requirements. As with any technology, it's important that the district keep all software up to date and remain on guard against suspicious activity. When in doubt, contact your IT department.

Please note: The Trust does not endorse any particular conferencing solution. Any product or service should be reviewed with your IT department to determine if it is appropriate and secure for district use.

Finally, please contact your member services coordinator if you have further questions.

Teleconference security tips:

- Require a meeting password or PIN for meeting sign-in.
- Identify everyone on the call. Meetings requiring registration will help with the identification process.
- Do not allow guest-initiated screen sharing. Instead, make sure the meeting settings require host permission before a guest can share their screen.
- Refrain from recording meetings that reveal confidential information.
- Ensure that all web conferencing applications on computers, phones, and tablets are updated frequently.
- Review all settings and turn off any defaults that are not needed for meetings (video, recordings, etc.). This will minimize unintended "surprises" during a meeting.
- If possible, use your phone for audio rather than your computer. Call quality is typically better, there is less delay, and it's easier to mute/unmute a phone than a computer.
- Cover the camera lens unless it's in use. Hackers can activate your camera without your knowledge.
- Carefully evaluate links that may be sent to you or others in the chat box. Don't open links from people you don't know and trust.
- Minimize use of other applications during meetings. This will reduce the chance of unintentionally sharing information that is not relevant to the meeting.
- End your meeting completely when it's over. Leaving a meeting open could result in unintentional information sharing.
- For improved security, ensure that employees' personal accounts (Facebook, Google, etc.) are not linked to their district accounts. If one of these accounts is compromised or passwords are leaked, the district's teleconference account becomes vulnerable.