ARIZONA
DEPARTMENT
of CHILD SAFETY

Mike Faust, Director
Douglas A. Ducey, Governor

April 15, 2020

Re: A message from DCS IT regarding Zoom Meetings

Dear DCS staff and providers,

Many of you are joining meetings through Zoom meetings and we understand it is a valuable tool to help with the current need for physical distancing.

Please use caution with this application as several vulnerabilities exist including misrouted data, "zoombombing" where uninvited individuals can take over a meeting, compromised accounts, cryptocurrency mining and malware.

For your consideration to mitigate these issues and practice safe Meetings!

- User's should only join meetings that have been determined as valid, for instance through a calendar invite received from a person's email known to you.
- All meetings should have a password to access and be set to private. It is more susceptible to "Zoombombing" if not.
- Do not click on links without knowing the legitimacy of them.
- Do not share confidential information using Zoom meetings.
- Verify only personnel invited to the meeting have joined. If a user(s) not invited to the meeting joins, leave the meeting immediately and ask for a new one to be created.
- Confirm all meetings before joining them.
- Do not post any links within the chat. If someone requests a link be sent, send it in a separate email.
- Do not put any confidential information within the chat feature. DCS does not have the capability to audit or remediate any issues within the chat.
- Do not download any attachments from the chat or meetings.

Thanks and Warm Regards,

Linda Roberts
Assistant Director | Information Technology
Chief Information Officer