Protecting Privacy/When Using Technology

Schools are finding free video conferencing capability a useful and effective means for accomplishing instruction and maintaining community during the government mandated closure caused by the COVID-19 virus. Some school leaders have expressed concern about student privacy when these tools are used, a concern that comes from reports that the interest that tech companies have in data collection will compromise student privacy.

Our schools, families and students are currently using platforms, mostly Zoom and Google Meets, for some synchronous aspects of the daily routines that have been established. These purposes include, for example, direct instruction, daily check-ins, and teacher meetings. There are best practices for these kinds of instructional and meeting uses that should be followed when using this technology.

The following controls are available through the technology and should be used to moderate the conference:

- Disable "Join Before Host" so people can't join and begin before you arrive
- Disable "File Transfer" so there's no malicious file sharing between computers
- Disable "Allow Removed Participants to Rejoin" so booted attendees can't come back in
- Do not post the Zoom conference link in any public profile, website, link, etc.

The following procedures should be followed when setting up conferences with students and parents and can be adapted for different age groups as appropriate:

- Receive parent permission prior to scheduling any conference
- Include parents in email communication and the meeting itself, especially with younger children
- Include a second teacher, administrator or aide on the conference
- Record the conference

Additional information relative to the mentioned platforms as well as other platforms can be found on the following two pages.

Additional Information

Google and Meet offer FERPA and COPPA compliant security and have reasonable strong end-to-end encryption in place for security. They offer many settings that would allow end users to opt-out of participating in videos, and both platforms allow for recording meetings, which should be required in most situations. Security is only as strong as the user.

Summation

- Both platforms have a strong level of encryption
- Only Google for Education accounts have stated FERPA/COPPA compliance.
- Zoom's documentation says it is compliant, but is vague about which account types that applies to
- Most of the compliance issues have to do with
    - Making sure that participants know they are being recorded
    - Have the right and ability to opt-out
    - Both platforms have this ability
- Best Practices for these platforms for our educators to use in every meeting to apply the strongest security possible.

- Every session, at least as far as classroom meetings, should be recorded.
- These recordings need to be stored where the school can control them. (Particularly if a parent asks that the recording be deleted, within their rights under the applicable FERPA/COPPA rules.)
- Recordings are published in a way that keeps the content private within the school/classroom. Teachers shouldn't be posting content up on public YouTube channels, etc.
- Parents should be aware when recordings happen and what their rights are as far as letting their students opt-out of live recordings.
- Students should be reminded that recording from their end is covered under school policy, just as if they were in school. Which generally means they aren't allowed to do it. Hard to enforce, but it should be said.
- Monitoring and communicating with teachers about security issues will need to be ongoing.
- Limit platform choices to one or two.

Google for Education and Zoom Features

- Both platforms offer end-to-end encryption, with some exceptions
  - Calls to actual phones may not be encrypted if the telephone provider can't provide that functionality
  - If a user is using a third-party add on, like special hardware in a conference room, the video might not be encrypted onto that hardware/application. This would be an unusual circumstance for WFH – Distance Learning
- Both platforms allow for
  - Controls over who can record video, so that only the organizer can start videos
  - Chat or audio only meetings
  - Participants in the meeting have control over their audio and video settings so they can choose to self-mute or not show video

Google

- Meet and Hangouts are covered under the security policies as the rest of the GSuite, which is FERPA compliant.
- GSuite administrators can set some security settings as default, such as only allowing meetings with members with a school email address. Good to keep participants inside the school, problematic if they want to use this platform with parents.
- Google administrators can see chat and Hangout logs through the admin dashboard.

Zoom

Exploring about whether they are going to apply their FERPA standards to basic accounts opened by educators. They know which ones are educators' accounts, which is how they unlock the accounts for unlimited meeting length. But right now, you have to assume they are applying Basic security standards to these accounts.

- Zoom for Education has full FERPA and COPPA compliance. The problem is that it is unlikely any school has this. This is expensive, and given that they are giving away basic with unlimited meetings...
- The platform allows for more security settings, including setting password for meeting, adding more encryption choices, etc.

- Meeting organizers can dismiss individual participants from the meetings. Google Meet doesn't have this control.

In addition:

Look at what other applications your teachers are using right now that have audio/video recording. There have been so many applications that are offering free upgraded version right now. Many of the Best Practices for Zoom, Meet, etc. would apply to these. These other applications might not be as secure as Zoom and Meet.