



Best Practices for Student Privacy





Let's help protect student privacy while we teach remotely - and actually, always!

So, do this...


...not that


screen names

 Have students use first name only (or a pseudonym) as their screen name and an avatar as their profile pic in digital platforms.


 Have students use their first and last names, and photos that show their faces.


posting screenshots

 Clearly communicate that taking screenshots or photos of video conference meetings is not allowed, especially when students are visible.


 Post, or encourage others to post, screenshots/photos of video conferences on social media or a public-facing website.


privacy policies

 Before using any new tool, refer to its privacy policy and/or terms of service; check to see if it is on the list of signatories for the [Student Privacy Pledge](#).


 Ask/require students (especially those under the age of 13) to create accounts for new digital tools that require them to enter personally identifiable information (PII) without parent consent.


sharing links

 Send video conference links (Zoom, WebEx, Google Meet) through communication channels to which only your class community has access.

 Post video conference links to public-facing websites or social media.

parental preferences

 Make sure you understand any privacy requirements/requests of students and their families.

 Assume all families are comfortable with their child's name, photo, or other information being shared.