Privacy & Security

Some educators and administrators worry about privacy risks when using Al-powered tools, particularly around biometric data, student privacy, and video recordings. Misinformation or a lack of understanding about how Sibme Al processes and stores data can increase hesitation.

Key Messaging

- Sibme AI tools are built with privacy first—our data is secure.
- We comply with all education privacy laws, ensuring student and educator protection.
- Educators remain in full control of their data. Al simply helps process what they choose to analyze.
- While adding your Biometrics to your Sibme profile can allow you to get more accurate Reports and Insights, they are not required to leverage all that Sibme AI has to offer.

Strategies to Address This Concern

- 1. Provide Transparent Al Privacy Information
- Share data security policies upfront.
- Explain that Sibme Al does not share or use biometric data.
- 2. Educate on Compliance with Privacy Laws
 - Highlight how Sibme aligns with FERPA, COPPA, and GDPR.
 - Offer documentation for district legal teams.
- 3. Offer Technical Solutions to Address Privacy
 - Provide <u>video blur features</u> to protect student identities.
 - Ensure Al-generated insights do not include personally identifiable information (PII).
- 4. Use Peer Testimonials & Success Stories
 - Show how other districts overcame privacy concerns.
 - Allow educators to hear directly from peers who successfully use AI while maintaining privacy.

