Administrator Privacy and Security FAQ for Cisco Collaboration for Education

Q: What is Cisco Collaboration for Education?
A: Cisco Collaboration for Education is Cisco Webex Meetings or Cisco Meeting Server and Cisco Webex Teams and optionally on-premises calling or Cisco Webex Calling ("Cisco Collaboration Services"). Click here for more information.

Q: How will students and teachers use Cisco Collaboration Services?
A: With Cisco Collaboration Services students will be able to communicate and work in groups to create, edit and share files and information for school-related projects with other students and teachers. Spaces in Webex Teams can be monitored by the school's administrators.

Q: Are there laws that protect children's privacy while using Cisco Collaboration Services?
A: Yes. The two main government acts that are in place to protect student data and privacy are FERPA and COPPA.

Q: What is FERPA?
A: FERPA is the Family Educational Rights and Privacy Act and is a Federal act that protects the privacy of student records. Click here for more information about FERPA.

Q: How does FERPA apply to Cisco Collaboration Services?
A: FERPA compliance is the responsibility of the school district offering Cisco services to faculty and students. To ensure student education records remain private, they should not be stored in Cisco Webex Teams or shared over Webex Meetings or Cisco Meeting Server meetings.

Q: What is COPPA?
A: COPPA is the Children's Online Privacy Protection Act. COPPA imposes requirements on operators of websites or online services directed to children under 13, and on operators of other websites or online services that have actual knowledge that they are collecting personal information from a child under 13 years of age. Click here for more information about COPPA.

Q: How does COPPA apply to Cisco Collaboration Services?
A: Cisco Collaboration Services are online services and are available via a web interface. Per COPPA, students under the age of 13 must have parental or guardian consent prior to using online services. Parents or guardians must read and agree to the Cisco Privacy Policy, the Cisco Webex Service Privacy Data Sheet, and the Cisco Webex Meetings Privacy Data Sheet on behalf of the child prior to use. The school districts deploying Cisco Collaboration Services are responsible for providing notices to and obtaining consents from parents/ guardians prior to collecting, using and processing student personal information so that Cisco can deliver services. Parents/ guardians should have the ability to request, access, correct, delete, or suppress the personal information collected from the minor children.

Links to policies and supplemental documents:

- Cisco Privacy Policy
- Cisco Webex Service Privacy Data Sheet
- Cisco Webex Meetings Privacy Data Sheet

Q: What is CIPA?
A: CIPA is the Children's Internet Protection Act that imposes two additional certification requirements for schools who receive discounts offered by the E-rate program:

1) Internet safety and monitoring policies of minors; and
2) Education of minors about appropriate online behavior. For information visit this website.

Q: How does CIPA apply to Cisco Collaboration Services?
A: If CIPA applies to your school, you must implement Internet safety policies as outlined by CIPA as Cisco Collaboration Services are online applications.

Q: Who has access to student personal data?
A: The administrators who oversee Cisco Collaboration Services will have access to student personal data used to set up student accounts. This personal data is shared with Cisco to allow access to Cisco Collaboration Services. To learn more about what Cisco defines as personal data and how it handles shared personal data, consult the Cisco Online Privacy Statement, the Cisco Webex Service Privacy Data Sheet and the Cisco Webex Meetings Privacy Data Sheet.

Q: Who has access to the content a child posts in Cisco Webex Teams?
A: School administrators can set up Cisco Webex Teams so that only students and teachers within the school can view posted content. Learn more.

Q: Are conversations and documents shared in Cisco Webex Teams secure and private?
A: Yes. Industry-leading end-to-end encryption ensures all messages and content remain secure and available at all times. With Cisco Webex Teams, your data is secure and private.

Q: Who is responsible for securing parent/guardian consent?
A: School districts are responsible to secure parental/guardian consent.

Q: What resources does Cisco provide to schools that help parents understand and consent to the use of Cisco Collaboration Services by their children?
A: Cisco provides a sample parental consent form that can be tailored to meet your specific use/need to obtain consent for minor's use of Cisco software. Cisco also provides a parent friendly FAQ to help schools address parental questions. Visit the Sample Parental Consent form, and the Parent Frequently Asked Questions.

Q: Where can I find a high-level overview of Cisco Webex platform security, compliance and management functionality?
A: Please click here to learn more.

Q: How are Cisco Collaboration Services managed?
A: The Cisco Webex Control Hub is a web-based tool for full visibility and control across the Cisco Webex service including Cisco Webex Meetings, Cisco Webex Teams, and Cisco Webex Calling. Webex Control Hub is the gateway for provisioning, administration, and analytics. It also provides a dashboard for usage and performance across the whole cloud service. There is Pro Pack for Cisco Webex Control Hub available as a premium add-on for customers that require more advanced capabilities. For complete details on Cisco Webex Control Hub and Pro Pack visit this link. Optionally, Webex sites can also be managed by Cisco Webex Site Administration.

Cisco Meeting Server is managed by Cisco Meeting Management. Using Cisco Meeting Management, administrators can easily manage security, auditing, account management and permissions, diagnostics and troubleshooting, and monitor and control meetings (add, drop, or mute participants, change layouts, start or stop recording or streaming, etc.). For complete details, click here.

On-premises calling is managed by Cisco Unified Communications Manager. For complete details, click here.

Q: How can teachers and administrators monitor all conversations and content in Cisco Webex Teams?
A: Teachers and administrators can set up team spaces for student work groups and can enter in and out of spaces to monitor activity and messages. Additionally, an eDiscovery tool is provided via Cisco Webex Control Hub to generate reports on content even in Webex Teams spaces teachers or administrators are not directly part of.

Q: How can administrators ensure Cisco Webex Teams messages between individuals are appropriate and in accordance with school policy?
A: Cisco Webex Teams can be integrated with third party Data Loss Prevention software solutions that can look for key words, phrases or content and automatically take action based on policy settings.

Q: Can administrators use Cisco Webex Control Hub to set content archival periods?
A: Yes. Security or compliance officers can define compliance settings for retention, conduct eDiscovery, and integrate with existing compliance software to align with school InfoSec policies.

Q: Can compliance officers access students deleted messages to address in-appropriate use of Cisco Webex Teams?
A: Yes. Deleted messages are managed in accordance with education institution's retention policies and can be archived for a pre-determined period of time. An eDiscovery tool is provided via Cisco Webex Control Hub to generate reports. Messages can also be off-loaded using API functions and can be stored on-premises if required.