SECURE VIDEO CONFERENCING FOR NGOS

JUNE 2024

DISCOVER THE SAFEST TOOLS FOR YOUR VIRTUAL MEETING ROOM

www.righttoconnect.org

RIGHT TO CONNECT
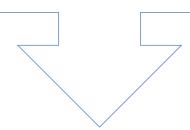
Table of Contents

Disclaimer:

The opinions expressed herein are those of the author(s) and do not necessarily reflect the views of our donors and RTC. While RTC retains the intellectual property rights of these guidelines, individuals and organizations are authorized to use, reproduce, and distribute any part of this material solely for non-commercial, educational, or scholarly purposes, provided that the use is accompanied by an acknowledgment of the copyright holder's name and a citation of the original source.

Our Facebook   *Our LinkedIn*   *Our Twitter/ X*   *Our Instagram*

What are the safest video conferencing tools for NGOs?

Apart from a few, none of these video conferencing tools are completely secure. Select them based on your communication sensitivity.

THE SAFEST VIDEO CONFERENCING TOOLS FOR NGOS

Tool	Encryption sensitivity	Data Privacy	Security Features
Jitsi Meet	Provides end-to-end encryption for video conferences and ensures secure communication channels.	Open-source platform with no cost, and users can self-host servers for added privacy.	Password-protected rooms, same-room participants visibility control, and user password authentication.

Website:
https://meet.jit.si

Tool	Encryption sensitivity	Data Privacy	Security Features
BigBlueButton	Supports encrypted web traffic and includes security features for maintaining confidentiality.	Designed for educational contexts, it provides controlled access to recordings and features.	Selective access permissions, moderation controls, and virtual whiteboard collaboration tools.

Website:
https://demo.bigbluebutton.org

Tool	Encryption sensitivity	Data Privacy	Security Features
Whereby	Offers end-to-end encryption for calls and meetings conducted on the platform.	Provides the ability to set passwords for meetings and control access to them.	Secure, password-protected virtual meeting rooms and waiting room features.

Website:
https://whereby.com

Tool	Encryption sensitivity	Data Privacy	Security Features
Blue Jeans	Provides encryption at rest and in transit to secure user data during calls and conferences.	Offers privacy features like data masking and controlled participant permissions.	Secure join features, privacy controls, and moderator controls for meeting security.

Website:
https://www.bluejeans.com

Tool	Encryption sensitivity	Data Privacy	Security Features
GoToMeeting	Uses strong encryption protocols to secure data during calls and conferencing.	Compliance with data protection regulations, but user data may be collected for service improvement.	Meeting lock feature, screen sharing restrictions, and attendee access permissions.

Website:
https://www.goto.com/meeting

Tool	Encryption sensitivity	Data Privacy	Security Features
Facetime/i Message (Apple)	End-to-end encryption for texts, calls, and video chats within the Apple ecosystem.	Strong privacy protections due to Apple's encryption standards and commitment to user privacy.	Blocked contacts, Face ID/Touch ID authentication for apps, and automatically expiring iMessages.

Website:
https://support.apple.com/en-ca/guide/deployment/dep154cd083a/web

Tool	Encryption sensitivity	Data Privacy	Security Features
Google Meet	Provides secure video conferencing with end-to-end encryption in transit and at rest for all G Suite users.	Google's security standards ensure data protection, but user privacy might be impacted by data collection for personalized ads.	Meeting lock, privacy controls, and measures to prevent unauthorized access.

Website:
https://meet.google.com

Tool	Encryption sensitivity	Data Privacy	Security Features
Duo (Google)	Uses end-to-end encryption for calls and video chats, securing communication from third-party access.	User data collection for service improvement might impact privacy, alongside meeting Google's security standards.	Encrypted video calls that prevent the interception of communication, Face Match for authentication.

Website:
https://meet.google.com/calling/

Tool	Encryption sensitivity	Data Privacy	Security Features
Microsoft Teams	Secure transmission and storage of data with comprehensive encryption protocols.	Complies with strict data privacy regulations with advanced privacy settings and controls for users.	Encrypted communications, multi-factor authentication, secure channels, and compliance standards.

Website:
https://www.microsoft.com/en-ca/microsoft-teams/log-in

Tool	Encryption sensitivity	Data Privacy	Security Features
Xspace	Xspace provides end-to-end encryption for video calls and ensures secure data transmission during private space communication.	Highlights user data protection and ensures compliance with data privacy regulations.	Implements password-protected meeting rooms, admin controls for access permissions, and secure document sharing features.

Website:
https://twitter.com/

THE SAFEST VIDEO CONFERENCING TOOLS FOR NGOS

Tool	Encryption sensitivity	Data Privacy	Security Features
Clubhouse	Clubhouse faced criticism for its lack of end-to-end encryption, leading to privacy concerns regarding the security of audio chats on the platform.	Users have raised privacy concerns due to data retention practices and previous security incidents involving uninvited listeners joining private conversations.	Limited tools for moderation and control over conversations compared to traditional conference platforms, which could impact user safety.

Website:
https://www.clubhouse.com/

Tool	Encryption sensitivity	Data Privacy	Security Features
Zoom	Faced initial encryption controversies but has since upgraded its security protocols to provide end-to-end encryption for all meetings and messaging.	Improved data privacy practices and transparency following scrutiny, offering options for users to control data sharing and security settings.	Offers a range of security features like password protection, waiting rooms, host controls, and end-to-end encryption to safeguard user communication.

Website:
https://zoom.us/