Privacy Considerations when using Virtual Meeting and Collaboration Platforms

To ensure the protection of personally identifiable information and to meet privacy regulations requirements, special care needs to be taken when using virtual meeting and collaboration platforms ("virtual tools and technologies").

The following guidance is offered to you by the GW Privacy Office, in Collaboration with GW IT and it aims to assist in minimizing the risk of accidental personal information disclosure, while using virtual tools and technologies.

Faculty and Staff should only use virtual tools and technologies that have university approved contracts, as they are privacy compliant (through appropriate privacy terms and conditions) and configured with adequate security and privacy protections. To protect university non-public information, virtual tools and technologies should be integrated with GW Single-Sign On or two-factor authentication, as well as have the capability for event-specific password protection, encryption and attendance control.

In absence of a contract, virtual tools or technologies should not be used for any university activity where non-public information will be shared.

Information on available university approved virtual tools and technologies can be found on the GW IT Web Conferencing page. Additionally, virtual training and personalized guidance on tools and best practices for virtual learning can be found on the Tools for Instructional Continuity page.

Guidelines and Best Practices

To minimize risk of disclosure or breach of non-public data, these guidelines and best practices apply to virtual tools and technologies for **administrative operations and virtual learning.** Both the organizer (host) and participants should be aware of the privacy risks and exposures that exist when facilitating and participating in online meetings using virtual tools and technologies.

Be familiar with configurations and settings that minimize privacy risks associated with the use of virtual tools and technologies, such as the difference between public and non-public virtual meeting rooms:

- **Non-Public Meeting Room:** If the virtual event will contain content that is sensitive or includes any personal identifiable information (PII or PHI), a non-public meeting room should be used. A non-public meeting room is one where a one-time password or access code for entry into the meeting room is required; End to end encryption is strongly recommended. All available encryption and privacy modes should always be enabled. Do not record the virtual meeting unless it's absolutely necessary (e.g. for purposes of records retention or asynchronous learning.) If the meeting is recorded for asynchronous learning purposes, the recording must not be shared outside of the class roster without student consent.
- **Public Meeting Room:** If the content will not include any personal identifiable information (deidentified PII or PHI or general administrative or academic content), a public meeting room can be used. For example, a Webex personal room is a public meeting room unless a password has been enabled.

The following guidance applies to both **non-public and public meeting rooms**:

- Use a 'green room' or 'waiting room' to allow the meeting to begin only after the host joins.
- Carefully control and monitor who has the ability to invite/share the meeting invite. For example: avoid making the meeting available to anyone with the link.
- Monitor attendees through a dashboard – identify all generic attendees before meeting begins (e.g. Caller X). The host should pay attention to all new/late arriving attendees and ask them to identify themselves. An unauthorized attendee should be expelled or the meeting room may be locked once in progress to prohibit others from joining.

- Before anyone shares their screen, files or other content, remind them not to share sensitive or personally identifiable information during the meeting inadvertently.

Online Classes

Instructors should be aware of the privacy risks and exposures that exist when hosting online classes and lectures and maintain compliance with FERPA with regards to student's personal information captured via virtual tools and technologies.

Instructors should be familiar with configurations and settings that minimize privacy risks, such as controlling attendance by not making the meeting available to anyone with the link. When the online class invite includes a virtual conference link, ensure students do not forward the link to others not in the class, whether by mistake or otherwise.

Telehealth Activities

GW Clinics may seek to conduct telehealth activities. When using virtual meeting applications to provide telehealth services, all state licensing requirements and regulations for health professionals must still be met. If virtual meeting applications will be used for telehealth activities, non-public meeting rooms must be used. This requires the use of a one-time password or access code for entry into the meeting room. End to end encryption is strongly recommended. All available encryption and privacy settings should be enabled.

Recordings

As a general rule, meetings, events, classes, lectures or health sessions should not be recorded without a legitimate business purpose.

Meetings and Events | **Class Recordings** | **Telehealth Sessions** | **Storage and Retention**

Before recording a virtual meeting or event, you should notify attendees of your intent to record. Provide attendees with details about why you want to record the meeting or event, and ask their consent to the recording being used for that purpose. You may also consider giving attendees the option to participate without having their image and/or voice recorded, such as allowing them to attend with no video or audio, and the option to pose questions only in the text chat window.

Zoom AI Companion

Zoom AI Companion is now available to all GW Staff and Faculty. Click here for instructions on how to enable Zoom AI Companion for your university Zoom account.

Overview | **Privacy Considerations**

Zoom AI Companion uses AI technology to allow meeting hosts to initiate an AI-generated summary of their meetings and create smart recordings.
The **Zoom AI Companion Meeting Summary** uses artificial intelligence to shorten important meeting points into a brief summary. After the meeting, the host quickly gets an email with a detailed summary, including Quick Recap, Summary, and Next Steps sections.
Zoom AI Smart Recordings extends the capabilities of Zoom AI Companion to cloud recordings with transcripts. It enables meeting hosts to categorize their cloud recording into segments known as smart chapters, while highlighting important information and next steps.

Resources

- Web Conferencing at GW
- Online Teaching Guidance offered by the GW Instructional Design Team
- Blackboard

Contacts

Privacy Assistance	GW Privacy Office	Email us
Technical Assistance	GW IT Support Center	Phone: 202-994-4948, Email: ithelp@gwu.edu

GW Privacy Office

Email the Privacy Office

Report a Data Incident

Data Subject Requests