

# 2022-2023: Technology Basics - Information Security, Confidentiality, and Decorum



**Disclaimer:** This module is intended to provide a foundational understanding of the best practices associated with technology use during the administration of conduct and/or Title IX related grievance processes.

Public and private academic institutions and their respective campus community members use various technological systems, programs, and platforms to meet their basic needs, including email, secure information sharing, meetings, and virtual hearings. These system, program, and platform variations exist not only across different colleges and universities but sometimes among institutions within the same university system. Thus, it is important that confidentiality, information security, effective and efficient operations, and decorum remain institutional priorities despite the mechanisms used from a technological standpoint.

**Content Creators:**

Elizabeth Brady, Former Director of Sexual and Interpersonal Violence Prevention, SUNY

Mishka Woodley, Assistant Counsel, Office of General Counsel, SUNY

Michelly Peña, Interim Director, SCI

Created in July 2020

Updated June 2022

≡ Introduction

≡ Part 1: Preparation

≡ Part II: Logistics - Key Considerations

≡ Part III: Decorum

≡ Conclusion

# Introduction

---



All trainings and resources offered by the SUNY Student Conduct Institute (SCI) are the work product of the content creator(s) and presenter(s) reflected in the module descriptions and presentations. They are intended to provide educational content and advise on general compliance, as applicable. SCI training and resources shall not constitute legal advice and use of, and access to such, shall not create an attorney-client relationship. Please consult with your own attorney to obtain advice regarding all matters specific to your institution. We at SCI deeply value the opportunity to share invaluable educational content from our SUNY and nationwide experts with you through our on-demand and Live@Distance trainings and resources.



Complete the content above before moving on.

---

## Introduction:

# Technology Basics - Information Security, Confidentiality, and Decorum

## Objectives

This module will:

- 1 Identify ways to prepare to use different modes of technology throughout various phases of a conduct related grievance process to ensure effective and efficient processes.
- 2 Identify ways to address information security and confidentiality related issues.
- 3 Understand the importance and implications of proper decorum in various virtual settings.

## Basic Technological Needs

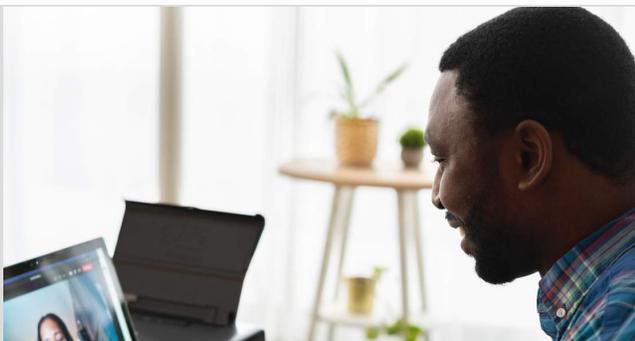
Public and private academic institutions and their respective campus community members use various technological systems, programs, and platforms to meet their basic needs. Based on the examples below, see if you can guess what the common technological needs are:



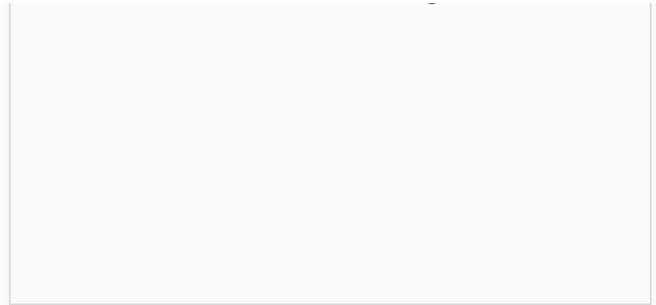
Communication via email



Secure information sharing



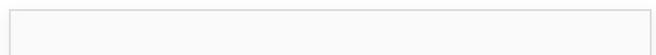
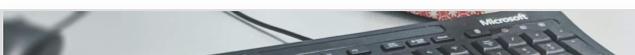
Private meetings



Virtual hearings or informal resolution options



Secure storage of files and recordings





Accessibility needs



Complete the content above before moving on.

## Technological Priorities and Research

Differences in technological systems and software exist not only across various colleges and universities but sometimes among institutions within the same university system. As such, consider where your institution stands with the below priorities for all mechanisms used from a technological standpoint.

- Effective and efficient operations
- Information security
- Confidentiality and privacy
- Access and accessibility
- Decorum

---

While various technological systems, programs, and platforms within the same category **generally have similar basic functionalities** and settings, each will be different. So, **it is important to appropriately research** any new technological systems and/or programs your institution intends to use systemwide or for specific programs, processes, or projects.

 Institutions should be cautious about “recommending” specific technological systems or programs to students for their academic or personal use without proper vetting by and receiving permission from your institution’s personnel responsible for overseeing tech specific matters and security.

CONTINUE

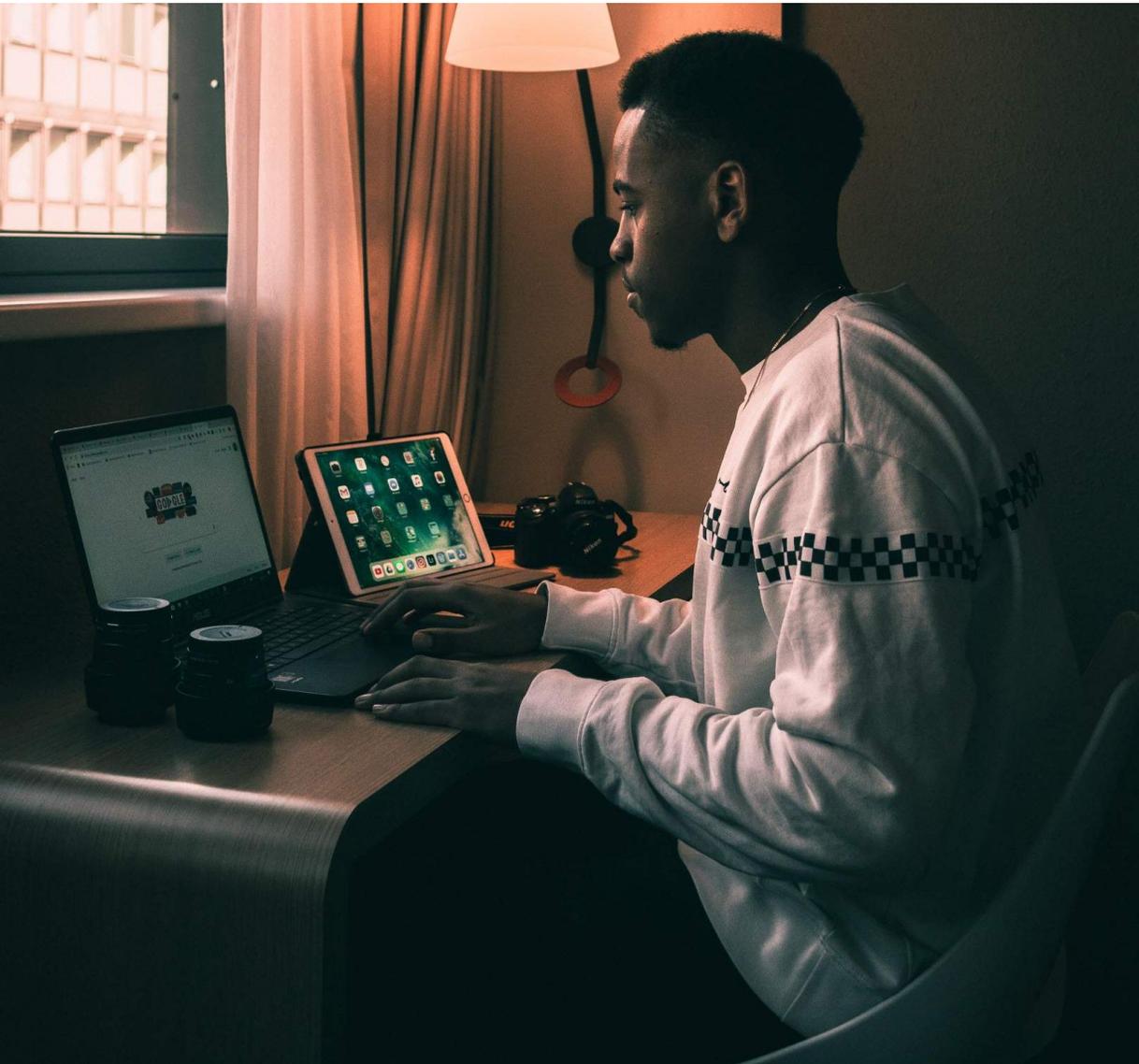


An image of an individual reviewing post it notes with ideas written on them.

---

Once you have learned the various technological resources your institution has identified to meet its need, it is important to understand the terminology and features of those specific resources to help you appropriately prepare for its effective and efficient use.

In support of your efforts, the Student Conduct Institute (SCI) has designed a reference list of web platform solutions and their features that is available in the SCI Toolkit entitled Virtual Hearing options comparison chart.



An image of an individual reviewing a website on their laptop.

---

**i** Please note, as a disclaimer, that you should be trained on the specifics of the technology that you use on your campus. Technological updates and customized products to meet institutional size and needs are common.

CONTINUE



# Part 1: Preparation

---

## Practice and Preparation for Technology Use

One of the most critical – but often forgotten steps – when using technology is **testing**. Generally, individuals have become so accustomed to using their respective systems and programs, and troubleshooting them when they fail to operate, that they forget the importance of verifying, testing, and practicing prior to use. The need to do so applies whether preparing and sending emails, facilitating file transfers, holding meetings, or executing hearings. You must ensure that the appropriate people have the intended access and capability to achieve whatever your desired outcome is upon first attempt whenever possible. These efforts include, but are not limited to, the following:

VERIFY CONTACT INFORMATION	INFORMATION SHARING	LOGISTICAL DAY-OF INFORMATION
-------------------------------	---------------------	----------------------------------

Double check to make sure that that contact information is correct.



VERIFY CONTACT  
INFORMATION

INFORMATION SHARING

LOGISTICAL DAY-OF  
INFORMATION

Confirm that information shared transfers appropriately when necessary and that security and confirmation mechanisms are in place.



VERIFY CONTACT  
INFORMATION

INFORMATION SHARING

LOGISTICAL DAY-OF  
INFORMATION

Making sure that individuals have the necessary call numbers, logins, website addresses and any other information necessary to execute necessary tasks or engage in an event or meeting. Consider scheduling multi-day meetings with multiple hour blocks to provide for set up time, breaks and other unanticipated issues. You can always cancel any time that isn't utilized.



**i** Once you have identified the technology you will be using, you need to plan for any logistical challenges that may arise, especially where virtual meetings and hearings are concerned.



Complete the content above before moving on.

## Test Technology

It is important to test all technology and troubleshoot any anticipated challenges with programs, equipment, etc. to be used a day or two before any scheduled meetings or hearings. A

few testing tips to consider:

<b>ADVANCED TESTING</b>	<b>TROUBLE-SHOOTING CHALLENGES</b>	<b>COMMUNICATION WITH TEAM MEMBE...</b>	<b>HELPFUL DOCUMENTATION</b>
-------------------------	------------------------------------	---	------------------------------

If time doesn't permit testing a day or two in advance, be sure that someone executes the testing process at least an hour or more ahead of time to provide time to address any last-minute issues. If the technology utilized is new, testing at least one day in advance is critical.



<b>ADVANCED TESTING</b>	<b>TROUBLE-SHOOTING CHALLENGES</b>	<b>COMMUNICATION WITH TEAM MEMBE...</b>	<b>HELPFUL DOCUMENTATION</b>
-------------------------	------------------------------------	---	------------------------------

As we all know, technological challenges are inevitable. Internet networks are slow, malfunction, or fail completely. Technological platforms and platforms may work intermittently. And technology users may not always be as savvy as we may hope, including ourselves. So, you must always have a plan in place if a file document wasn't received, systems get interrupted, or participants require extra assistance or behavior redirection. The key element of a mitigation strategy such as this is to communicate with students and participants ahead of time regarding what to do or who to contact if certain types of interruptions occur.

While you can't account for every issue that may arise, or behavior that individuals may engage in, identifying potential concerns ahead of time and making a good faith effort to address them is not only possible but very effective and worthwhile.



[ADVANCED TESTING](#)

[TROUBLE-SHOOTING  
CHALLENGES](#)

[COMMUNICATION  
WITH TEAM MEMBE...](#)

[HELPFUL  
DOCUMENTATION](#)

It is important to give any professional staff who are actively participating in or monitoring in the process the opportunity to test the equipment/technology as well.



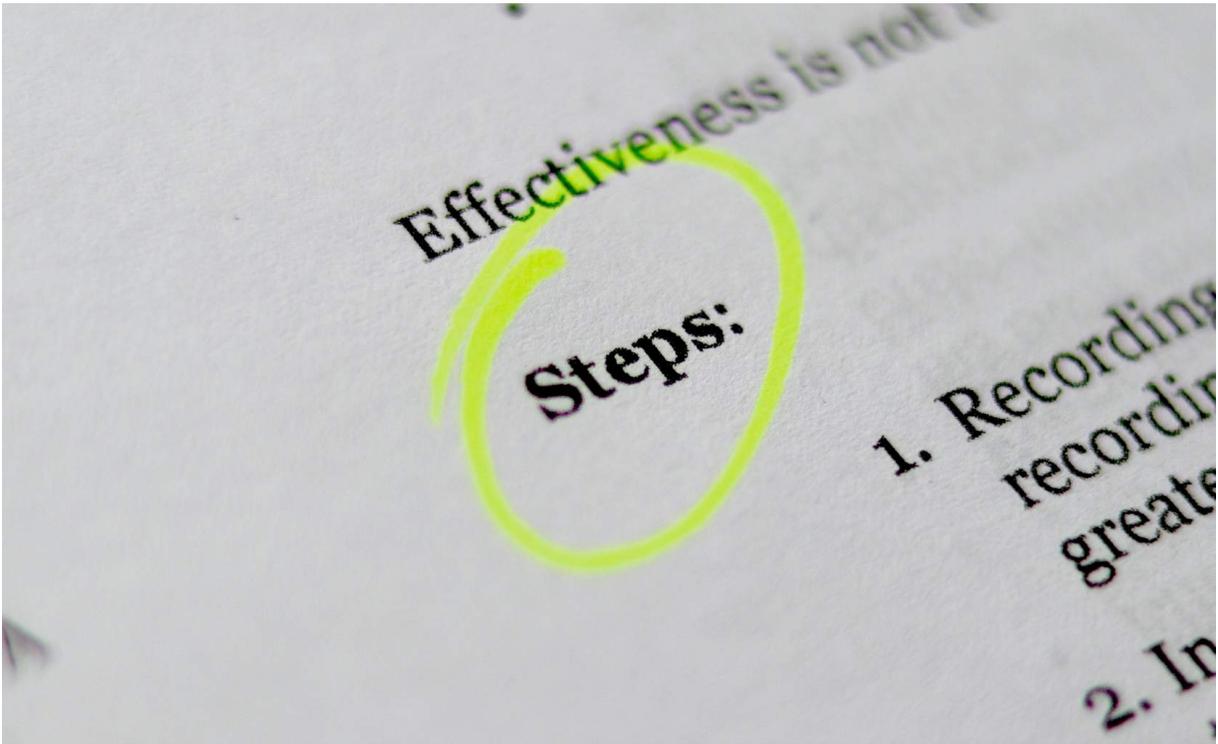
**ADVANCED TESTING**

**TROUBLE-SHOOTING  
CHALLENGES**

**COMMUNICATION  
WITH TEAM MEMBE...**

**HELPFUL  
DOCUMENTATION**

Consider creating and sharing an FAQ/guide for all parties that will be engaging with the technology over the course of the meeting or hearing as a resource to help facilitate a successful, worry-free experience for everyone.



Complete the content above before moving on.

## **Tech/User Services/IT Team Relationship Building & Outreach**

Develop a strong working relationship with your institution's user services or technology support office over the course of time.



An image of a group of individuals collaborating while utilizing their laptops.

---

1. Ask questions about how the institution's programs and systems work as questions or concerns arise.
2. Assess needs for your communications, file transfers, meetings, and hearings which must be secure and often timely.
3. Provide your tech teams with sufficient notice that support may be needed.
4. Plan for a practice testing day and invite technology support staff to assist.

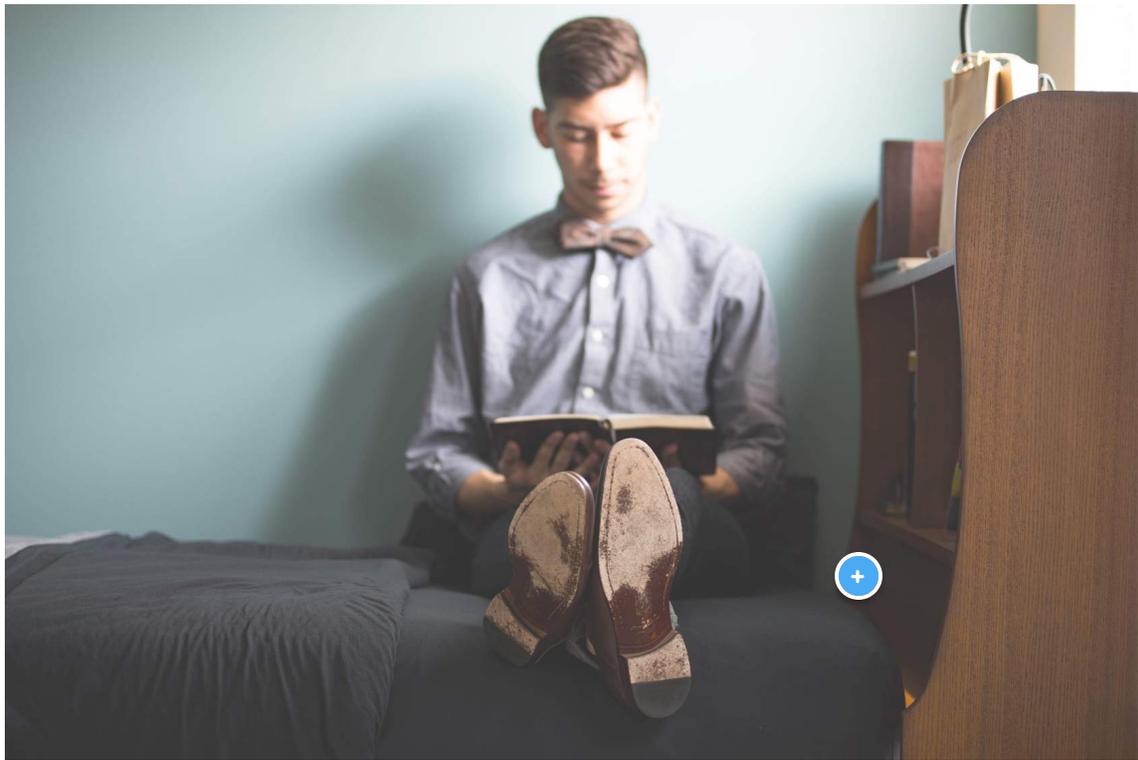
By laying a **strong foundation** of education and communication, you and your tech team will be **well prepared** to address **any issues** that may arise.

CONTINUE

## Student & Participant Outreach and Resources

Student conduct related processes can be a very stressful time for all parties involved -- especially students. Considering this, it is helpful to provide students with a preview of the process related to their specific conduct matter and what to expect. Consider the following when coordinating information sharing efforts:





### **Access to technology**

Students may have varying levels of access to technology and experience utilizing various systems and programs. Try your best to not make assumptions about students' level of access. Ask students whether they have any questions or concerns related to participating virtually.



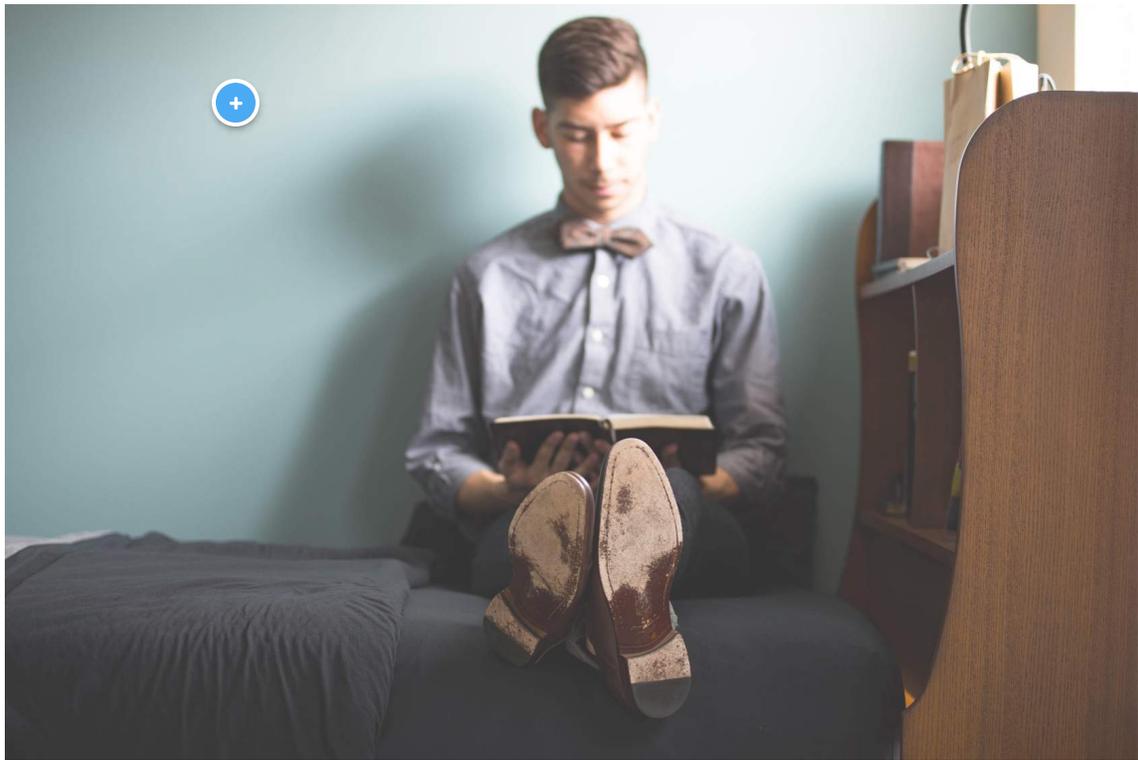
## **Accomodations**

Your outreach and policies may also help identify whether any accommodations otherwise unrealized are necessary.



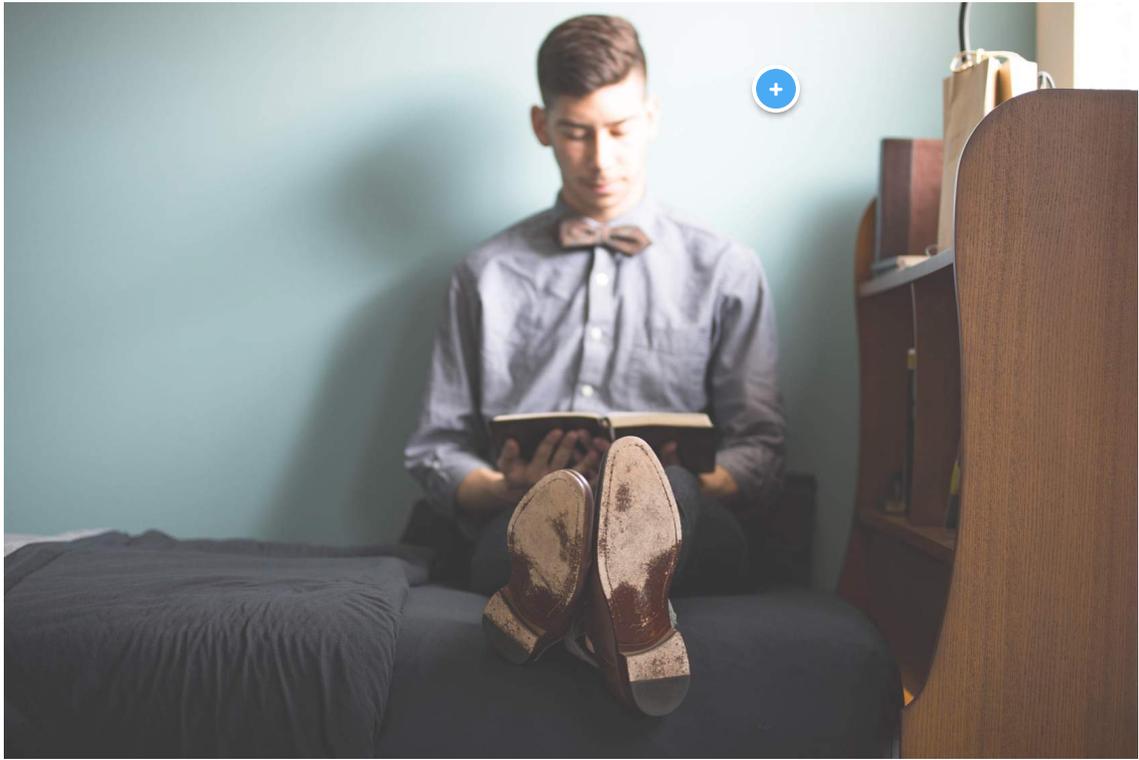
### **Provide a preview**

A detailed preview of the process related to their specific conduct matter and what to expect is helpful. Pictures and visuals can be helpful for visual learners.



### **Information sharing overview**

Consider informing students in advance of what information to expect electronically including communication correspondence and files shared. You can also inform students how they can best share information with you (e.g. large video files, large sets of images or texts, etc...)



### **Virtual meeting expectations**

Expectations related to virtual meetings or hearings that could take place.



## Privacy

Students have varying levels of privacy. Some students may share not only living spaces but technological equipment. Proactively engaging students early in any conduct process will ensure a more equitable experience as well as opportunities to provide options or resources as necessary.



### Troubleshooting examples

Review potential issues that may arise throughout the process and how participants can assist in troubleshooting those issues in an effective or timely manner (E.g. losing wifi connection or receiving a link that does not work properly).



Complete the content above before moving on.

### Additional Considerations:

1

Create an FAQ sheet or expectations guide, and update the language for your notification letters that go out ahead of time.

2

Provide students the option for a “tech run” prior to a scheduled virtual meeting or hearing.



3

Meet with Accessibility Services to discuss how to support an individual with accommodations.

4

Share IT/tech services information with students so that they can have any questions directly answered or they can troubleshoot issues if needed on their own.

5

Research interpretation services or what options exist within the platforms your institutions may already have access to.

**Regardless of which program or platform that you are using, it's important that functions such as file access and downloading authentication requirements, logins, screen sharing, chat expectations, reaction functions (e.g. Zoom has the raise hand function), mute/unmute, turn camera on/off, changing screen view etc. are fully understood.**

**It is important to also realize the limitations of these platforms and inform participants in advance of these limitations (e.g. communication with advisors who are not in the same location with the student). This preparation will enable students to feel more at ease with the process and will help to avoid unnecessary delays.**

**CONTINUE**

## Part II: Logistics - Key Considerations

---

### Communication: Emails, Files Shares, and Virtual Meeting/Hearing Invites

When sharing information, documents, or invitations for a meeting/hearing electronically, you want to ensure that sufficient information is included in any electronic communications or invites whenever possible. Consider the following:

File Sharing

If files are being shared, be sure that your communication, including the email subject, conveys to the reader that something of importance is enclosed or attached.

If the information is intended to be secure or

## Secure Information

confidential, include language stating such as clearly as possible.

## Privacy and Confidentiality

Some information may be difficult to be conveyed in writing. However, do your best to find a balance that is compliant with your institution's policies, requirements, and best practices.

## Shared Documentation Considerations

Consider whether content or documents can be read only, watermarked, accessible for a limited amount of time, etc.

Clear Instructions and  
Expectations

When individuals should refrain from sharing content, it is critical to clearly note disclaimers and share any potential violations/sanctions that could result from failing to comply with the

Meeting Agenda or Guide

Provide a meeting agenda or guidance related to the process whenever possible to establish a flow and reasonable expectation for the virtual experience ahead of time.

---

The goal is to ensure that the virtual meeting experience is as similar as possible to an in-person experience. Try your best to provide the same service as if everyone were to be live at the hearing in person.



Complete the content above before moving on.

## **Controlling The Privacy, Security, and Flow of A Meeting / Hearing**

Virtual conferencing technologies have meeting controls such as muting/unmuting participants that can help to control the flow of a meeting or the hearing.

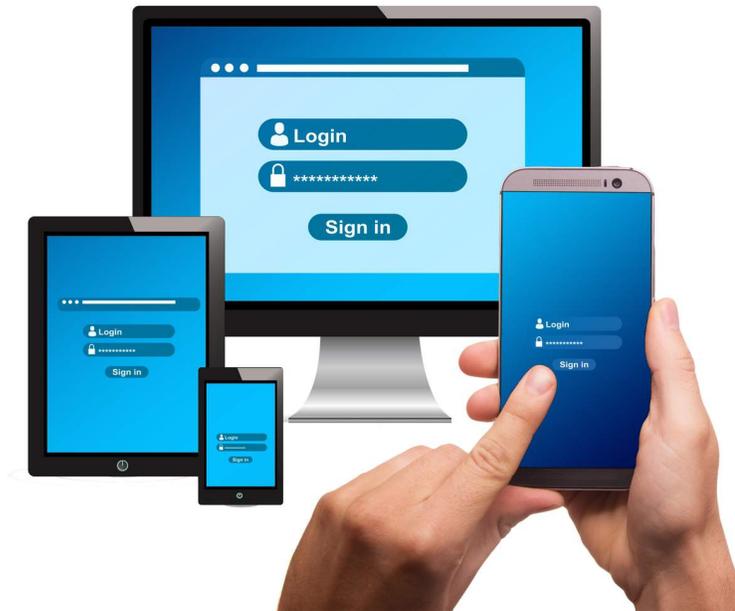
**A few tips...**



Consider establishing procedures for how the privacy, security and flow of a meeting work to ensure fairness, and who will be responsible for controlling these features.

## Tip # 1

# Passwords



Create and change passwords often, with the recognition that emails, and invites, can be easily forwarded, thus increasing risk of unapproved access to information and/or virtual settings.

## Tip # 2

### Emoji's or Chat Functions



It is also important to establish whether emojis or chat functions should be utilized in any fashion. If there is certain functionality that you want to limit, make every effort to disable that functionality ahead of time whenever possible to mitigate issues during the meeting.

### Tip # 3

## Security



There are also risks involved when using technology, which may include potential issues with security of the meeting, there are things to consider when working to make remote procedures more secure.

## Tip # 4

### Privacy



1. In person, it is easier to confirm who is physically in the room, in addition to when and how individuals are communicating with one another.
2. Think through how you can ensure that individuals are in a space that maintains privacy and confidentiality by reminding them ahead of time that they should not join a virtual session from a public space or a room where their family members or other third parties may be.
3. Remind them of the obligation of ethics and honesty. Remind them of any confidentiality requirements that might be applicable to the meeting or hearing at issue.

## Summary

Work with IT team members that you have developed strong relationships with to determine how best to put systemic and programmatic protections in place based on your specific needs.



Complete the content above before moving on.

**Other potential strategies for success that also prioritize information security and privacy include:**

Requiring meeting invite acceptance validation or pre-registration prior to the virtual event.

Enabling the waiting room to ensure appropriate screening for meeting/hearing entry prior to and during the virtual session.

Customizing waiting room messaging to communicate meeting expectations to facilitate participant compliance.

Limiting the number of dial-in options and/or requiring video only for virtual sessions if/when able and appropriate. (Note: Some sessions, such as hearings, may require that all cameras are on.)

Requiring professional business or institutional logins for confidential and/or secure communications and meeting invites.

Using official display names and titles for entry into and participation in meetings or hearings, as deemed appropriate.

Enable watermark features, if available, when screen sharing to mitigate inappropriate use and abuse of content shared electronically.

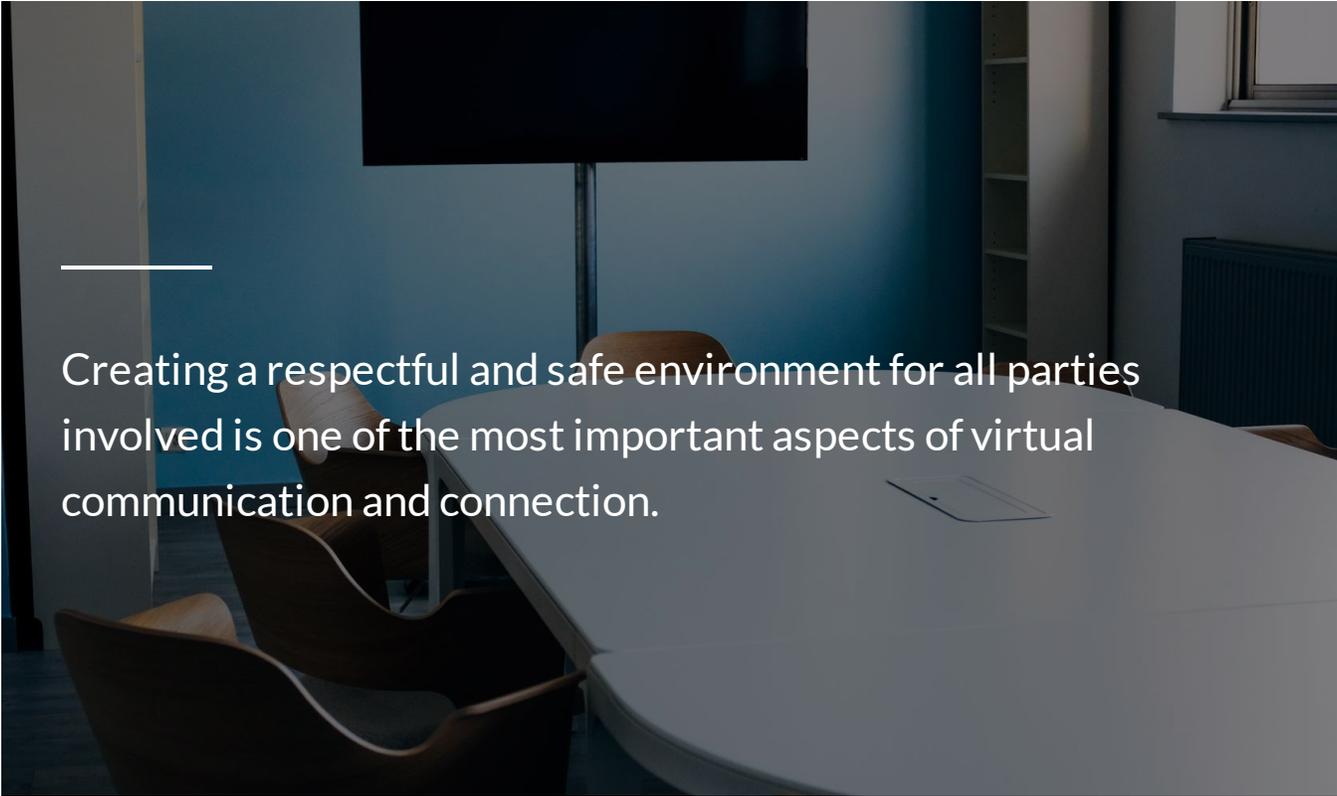
Turn off the virtual background function if/when necessary.

 While you may have controlled permission settings for recordings during virtual sessions, this doesn't mean that a student won't have access to third party software or external devices that could allow them to record. You need to remind students and all other participants about privacy regarding using third party apps and software or cell phones to record audio or video during a session, as applicable. Consult with your institution's policies and legal counsel to address any questions regarding the right to record and any other similar requests.

CONTINUE

## Part III: Decorum

---



Creating a respectful and safe environment for all parties involved is one of the most important aspects of virtual communication and connection.

### Decorum Tips

1

In your policies and during your meetings. It is important to convey rights and expectations surrounding the general tone and nature of communication that is permitted whether written, oral or visual.

2

Each institution should have their own respective policies and procedures surrounding expectations related to virtual engagement whether in the classroom, virtual meetings, social media, etc. Consult your institutional policies and procedures to ensure that your messaging aligns with that of your institution.



3

It is critical that any and all expectations be shared, prior to the opportunity for an incident to occur, to reduce risk of any allegations related to inequitable treatment.

4

Examples of Decorum referenced in the 2020 Final Rule include: 85 Fed. Reg. 30360-30361, see also, Id. at 30319 Institutions may “adopt rules of decorum that prohibit any party advisor or decision-maker from questioning witnesses in an abusive, intimidating, or disrespectful manner.”

If the manner in which an advisor attempts to ask the question is harassing, intimidating, or abusive (e.g., advisor yells, screams, or comes too close to a witness), the preamble explains that a school may enforce a rule requiring that relevant questions must be asked in a respectful, non-abusive manner (Id. at 30,320, 30,324, 30,342).



Visit the Title IX Toolkit for an example of a Model Decorum Policy that you can utilize.

CONTINUE

## Conclusion

---

---

**The ability to use technology to communicate, share documents, and connect virtually for meetings and hearings has significantly expanded flexibility and accessibility. When institutional systems, programs, and platforms are appropriately utilized, conduct and other related processes can be executed efficiently and effectively without undermining the student experience. If you keep efficiency, effectiveness, security, confidentiality, privacy, and decorum in mind, you can bring a more human touch to the virtual world.**

---

CONTINUE

## Thank you for taking this training!

Please make sure to select the "Complete Module" button at the bottom of this page. This will register that you have completed the module, and your progress will be uploaded into your learner dashboard.



Student Conduct Institute: The State University of New York

---

### Module Feedback Form

Please help us help your colleagues by providing feedback on this module. As always, your feedback is imperative to how we approach our work and your comments will help us to continue to deliver quality content to you and your peers.

FEEDBACK FORM

Student Conduct Institute Contact Info

Feel free to reach out to the Student Conduct Institute with any questions by clicking the button to send an email.

SCI EMAIL



Please select the "Complete Module" tab to finalize your completion of the module.

COMPLETE MODULE