<u>**Brookline Town Meeting Frequently Asked Questions**</u>

Where do I download the latest version of Zoom?
You can download the latest version of Zoom from the Download Center.

Why do I need to download the Zoom application?
The full set of features and functions, including polling, will be available to you if you install Zoom. And this method does not require a Zoom account.

Do you need an account to use Zoom?
A Zoom account is not required if you are strictly joining Zoom Meetings as a participant. If someone invites you to their meeting, you can join as a participant without creating an account. A Zoom account is only required if you need to create your own meetings and send invitations to participants.

Do I have to use a computer to join the Zoom Meeting?
You are not required to use a computer to join the meeting, however it is highly recommended due to the full features of polling available.

How do I join a Zoom meeting?
You will receive an email invitation, click on the Join Zoom Link in to register for the meeting. Please fill in your information, adding your title and precinct number to your last name so it displays in the meeting. Upon submission of your registration, you will receive an email to access the meeting. **NOTE:** A password is required for this meeting, but it will be automatically entered if you join by the post registration link. If you enter the meeting using the meeting ID, the password will be required. Learn more about joining a meeting.

How do I join computer/device audio?
On most devices, you can join computer/device audio by clicking Join Audio, Join with Computer Audio, or Audio to access the audio settings. Learn more about connecting your audio.

Do I have to have a webcam to join on Zoom?
While you are not required to have a webcam to join a Zoom Meeting or Webinar, you will not be able to transmit video of yourself. You will continue to be able to listen and speak during the meeting, share your screen, and view the webcam video of other participants. Enabling your webcam is highly recommended.

<u>**Security Frequently Asked Questions**</u>

What is "Zoom-bombing" and how does it affect my ability to conduct an online lecture privately with my audience?
The term "Zoom-bombing" refers to the ability of hackers to enter a Zoom session and take over the display or audio in attempt to disrupt and cause chaos. The host can take steps like

requiring a password, enabling the waiting room, and controlling who can share content that can help prevent intrusions.

On April 8, 2020 Zoom released an updated client for all platforms which adds a "Security" option to the host's in-meeting controls. This combines all of Zoom's existing in-meeting security controls into one place and includes locking the meeting, enabling Waiting Room, and more. Users can also now enable Waiting Room in a meeting, even if the feature was not turned on before the start of the meeting. For more information, please see Zoom's support article.

Is Zoom sharing my information with Facebook?
It was discovered that the Zoom iOS application was sending analytics information (mobile operating system type and version, device time zone, device model and the device's unique advertising identifier) of users to Facebook when the app is installed and being used.
On March 27th, 2020, Zoom issued an application update in order to disable analytics data being sent to Facebook. If you have not updated the application for iOS, please do so as soon as possible in order for this update to take effect.

When I use the Windows version of Zoom am I exposing my login and password information?
The answer is "no" however a security researcher has discovered that attackers can use the Zoom Windows client's group chat feature to share links in a way that will leak the Windows network credentials of anyone who clicks on them. Because of this, you have to be wary about clicking on links within a chat. Before you click, verify within the meeting that the link is credible and sent by someone within the meeting.

Zoom is currently aware of the issue and released an update on April 2, 2020. Please update your Zoom app to the latest version.

I heard that there was a discrepancy with Zoom's end-to-end encryption and its validity. Is my meeting information private and encrypted?
Zoom meeting information is fully encrypted when all parties are using the Zoom application. In a meeting where all the participants are using Zoom, and the meeting is not being recorded, Zoom encrypts all video, audio, screen sharing, and chat content at the sending client, and does not decrypt it at any point before it reaches the receiving clients. In this scenario, where all participants are using the Zoom app, no user content is available to Zoom's servers or employees at any point during the transmission process.

In scenarios where non-supported device such as a landline phone or a room-based system (think hardware used in boardrooms to facilitate meetings) which do not directly use Zoom, encryption as detailed above cannot be applied to that phone or device.

Etiquette Best Practices
These are general recommendations only.

Turn on Camera
- Check room lighting; make sure sources of light are not behind you. Lighting from the front is best.
- Meeting discussions are most productive when everyone's camera is on. It allows for more engagement and understanding.

Turn microphone off when unneeded
- To prevent accidental disruption on your part or from background noise, mute your microphone when entering the call.
- You should wait until prompted by the host to unmute yourselves for asking/answering questions.
  - If there is another person in the room connected to the meeting, please have them mute while you're speaking. They may need to stop their audio as well.
  - If you're watching the TV broadcast, please mute the TV when you speak.
- This prevents confusion due to crowded audio.

Don't spam or clog up the main chat
- The group chat feature of Zoom will only be used for official questions, points of order, or comments. Please do not hold informal conversations here (this is a meeting requirement).

Please contact ithelp@bu.edu or 617-353-1155 for support