Access to Academic Computing Resources and IT Guidelines for Remote Students Fall 2020

Accessing Software

Students taking courses remotely this fall will find some course software available through direct download. Other software will be accessible using the Tufts Virtual Desktop Infrastructure, or VDI. The VDI acts as a virtual computer lab and allows students to access Tufts-licensed software from Tufts servers on their own personal computers. For more information on VDI and how to set it up, please visit the TTS homepage at https://it.tufts.edu/guides/tufts-virtual-lab-vdi/tufts-virtual-lab-vdi

- A complete list of software available to students and directions for accessing each package can be found here: https://it.tufts.edu/technology-students
- VDI is available to both Mac and PC users.
    - TTS strongly recommends students and faculty install and use the VM horizon client to access Tufts VDI as it renders the most consistent display / printing experiences across many devices.
    - To successfully access the VDI, students will need their own computer running Windows 10, MacOS High Sierra (10.13) or later, or Linux (Ubuntu recommended).
    - Please note, if the internet connection is slow, some applications on the VDI may render slowly.

Maintaining Security and Privacy

Students should use the Tufts Virtual Private Network (VPN) for all course work and communications when outside the United States. More information on Tufts VPN can be found at this address: https://access.tufts.edu/vpn

- The Tufts VPN encrypts network communication as it travels between one computer and another. Network communications using the Tufts VPN are routed directly from the computer of origin to the Medford Campus network.
- VPN makes internet connections from all off-campus locations indistinguishable from those that originate on any of our campuses. This allows remote access to resources restricted to the Tufts community and provides a layer of security that mitigates (but does not eliminate) risks of network traffic surveillance.
- Tufts uses Cisco AnyConnect as its VPN – an industry leader. However, students studying abroad may find that international connections in some countries are blocked or slowed by state authorities.

Special Privacy Considerations

While VPN provides industry-leading encryption, it does not protect against all surveillance. Students studying from countries with pervasive government surveillance, in particular, should work under the assumption that their material may be captured and viewed by government authorities even when using the secure connections and/or the Tufts VPN.

Tufts Technical Support (TTS)

Students can receive technical support for software installations, VPN setup, and remote access by contacting the TTS service desk by emailing it@tufts.edu or calling 617-627-3376. TTS is available 24 hours a day, 7 days a week to students.

Important Considerations on Privacy

Students studying remotely in countries that invasively monitor their own citizens are vulnerable to surveillance of their online activities. There is no way for Tufts to guarantee that course information provided by students working in such countries will be secure and private. Students communicating from such countries should not have any expectation of privacy for their online activities even when using the Tufts VPN. While Tufts does not disclose its data to foreign countries, it is possible that information written or discussed online will be captured by governmental authorities through monitoring of in-country network communications and/or other means. Students should use care and be cognizant of local laws and customs when working online and assume that government authorities may gain surreptitious access to their communications.

Typically, the most vulnerable points in Internet communications are the computers being used at either end of an exchange. Students are strongly advised to reduce chances of being subject to malicious software by ensuring that their devices are kept up-to-date and that they only download software from reliable sources. For a check list of best practices, please review recommendations posted here: https://access.tufts.edu/student-computer-recommendations.

Privacy and Zoom

Zoom no longer routes connections originating in the US through other countries. Since Tufts VPN connections from other countries are treated on the network as if they originate at Tufts, students in foreign countries are provided with some measure of risk mitigation. Consequently, the most effective privacy protection for students studying abroad starts with connecting Tufts VPN and using Zoom to participate in class sessions. Under Tufts VPN, for example, Zoom sees a connection from a student in China as originating from Medford and will by-pass data centers in China. Even when following these recommendations, however, students working in privacy-challenged countries cannot assume that any form of online communication is completely secure. And if students use a personal Zoom account other than their Tufts account, or do not use Tufts VPN, we can make no guarantees that network activity will by-pass data centers in China.

Class Recordings and Privacy

It is essential for the privacy of all students that access to recordings of class sessions is restricted so that only the students and instructors in that class can view them. In cases where students studying in politically restrictive countries are recorded participating in discussions about sensitive political topics, consider making those recordings available to the class only when students need to access them and keeping them offline at other times. Instructors should take great care in setting access permissions when uploading Zoom recordings and making them available on their course websites.

Faculty that require additional guidance on any topic covered in this advisory should email edtech@tufts.edu.