Tufts Technology Services (TTS)
Securely Working with Technology
Especially Working Remotely or Using a Personal Device

Purpose and Scope
This document describes actions you can take to protect Tufts information and resources. By reviewing this document, you will become familiar with the University's expectations and best practices when using or accessing Tufts computing resources and/or Tufts data.

This document covers the use of both Tufts provided and managed devices and personally owned devices when working on or off campus. Note, this document does not specifically address expectations when travelling, whether domestically or internationally, or when working remotely from outside the United States.

Important: Central Administration and School Administrators must use Tufts owned computers that are managed centrally by TTS for accessing and performing Tufts work that involves institutional information except as follows when:

- Working with data that is defined as public data or
- You are only accessing your own personal information or
- Accessing your Tufts email & calendar (See "Access and Use Email" in section 5 below)

For emergencies when a Tufts owned-TTS managed device is not available, TTS has a loaner laptop program. On an infrequent basis, personal devices may be used in conjunction with the TTS virtual desktop service.

Overview of Document Sections
Key TTS Services
1. Key TTS Services for working on and off campus

Technology Device Expectations & Usage
2. Using Tufts Provided -TTS Managed Laptops and Tablets
3. Using Personally Owned Laptops, Desktops, Tablets, Phones and Other Devices
4. ALL DEVICES: Laptops, Desktops, Tablets, Phones, and other Devices whether Tufts Provided or Personally owned

Access & Data Management
5. Accessing Tufts Services – Using the Tufts Network
6. Data Management
7. Selling, Transferring or Disposing of any Device: A Laptop, Desktop, Tablet, Printer, Copier, Scanner, Fax Machine, USB stick, and External Hard Drives

Reporting Incidents with Security Implications
8. Reporting Lost Devices and other Security Incidents

Your Responsibilities
When working remotely with Tufts information or resources, you are responsible for your working environment including using technology appropriately. You are responsible for protecting Tufts data and systems and for complying with all related laws and regulations and University policies, guidelines, licenses and agreements. You are also expected to routinely monitor university communications on policy changes and comply with changes in all applicable policies and guidelines.

The policies you are required to follow include, without limitation, the Business Conduct Policy, Information Stewardship Policy, Use of Institutional Systems Policy, Data Classification and Handling Policy, and Information Roles and Responsibilities Policy, Email Policy, Box Use Guideline, Cloud Computing Services Policy, and Records Policies and Guidelines. You are also responsible for following any policies or guidelines your unit, school, or office has developed that may place additional restrictions on the devices and services you use, if you can perform that work off-campus, and/or using personally owned devices.

The **TTS SERVICE DESK** may be reached 24 hours a day, seven days a week at 617 627-3376 (preferred) or it@tufts.edu.

Key TTS Services

1. Key Technology Services for Working On and Off Campus	
The TTS website at it.tufts.edu provides links to access Tufts' full range of technology services and includes practical guides on how to use them.	
❑ Jabber	Make calls by VoIP using any computer or mobile device
❑ Microsoft Teams	Chat (instant messaging) using any computer or mobile device
❑ Zoom	Host and attend audio and video conferences, presentations, and meetings.
❑ Outlook Web App	Access email, calendar and other Outlook features
❑ Microsoft Office 365	Word processing, spreadsheet, presentation, and email software suite available for free on up to five computers plus five tablets or mobile devices
❑ tufts.box.com	Store, backup, access, and share content securely. See Tufts Box Use Guideline for permitted uses and Box Use Guide.
❑ **Service Desk Remote Assistance**	Enables the 24x7 Service Desk access to your computer remotely to resolve problems. Call (617) 627-3376
❑ Access Tufts	Access everyday administrative tasks in one place
❑ Tufts Virtual Desktop	A secure virtual computer that allows users to perform Tufts work from a personal device or to use specialized software
❑ Tufts VPN	A secure and private connection to the Tufts network from off-campus
❑ CrashPlan	A data backup service staff can purchase through TTS for those who do not use Tufts.box.com (free) for their data storage.
❑ TTS Laptop Loaner Program	TTS offers a laptop loaner program for those in temporary need of a computer for work or when traveling

Technology Device Expectations & Usage

2. Tufts Provided-TTS Managed Laptops and Tablets
All Central Administration, School and Clinic Administrators are required to use Tufts owned-TTS Managed laptops. If you require a tablet to perform work duties beyond accessing email you can request a TTS managed tablet. See the later section on usage guidelines for personally owned devices. Laptops and tablets will come prepared with the standard suite of software, appropriate security controls, and TTS central management and security tools.

How do I know if my device is TTS managed? TTS managed laptops and Tablets will have a Tufts asset tag applied to the outside of the device. If you are uncertain if your Tufts provided device is TTS managed, contact the TTS Service Desk after checking for the presence of the Tufts asset tag.	
❑ **Maintenance Responsibilities**	You are responsible for not disabling the TTS tools and processes and for ensuring the devices are able to connect to Tufts to routinely receive updates. Having your device managed by TTS significantly reduces your device management duties. If the Tufts managed device is not being properly maintained, you are responsible to work with TTS Service Desk to resolve the issues.
❑ **Usage**	You are allowed occasional, limited personal usage of the TTS managed laptop as long as it does not impact the security or performance of the device, Tufts network, or services. You are NOT allowed to let any non-Tufts person use the laptop
❑ **Use a Strong Password**	Use a strong, unique password to log into the device and protect your login/password by not sharing it with others. Use a password manager. See Tufts Password.
❑ **Manually Lock your Screen or Power Off every time** you leave your computer	Every time you leave your computer unattended, either turn it off or activate the screen lock that requires you to enter your password to resume working. See Screen Lock.
❑ **Keep Automatic Screen-Lock**	Tufts managed devices are configured for automatic screen-locks after a set number of minutes of inactivity. If your Tufts device is not so configured, re-enable it or contact the TTS Service Desk for assistance.
❑ **Don't Change Standard Privacy Settings**	When configured, Tufts managed devices have privacy settings limiting sharing to the minimum necessary. These settings limit applications' access to your location, contacts, calendars, and reminders. It is recommended you keep these settings to the minimum necessary.
❑ **Apply Patches and Updates** • For OS and Tufts provisioned applications • For browsers and applications not provisioned by Tufts	Tufts provided and managed devices are configured for automatic updates of the Operating System (OS) and Tufts provisioned applications whenever possible. Users are responsible for following prompts for updates as they are released and for following any prompts to reboot a device following an update to ensure proper functionality. For browsers and other applications you've installed, you are responsible for having all critical security updates applied and kept up to date with all new security updates as they are released. Updates for most products can generally be found by going to the company website and searching for "security updates."
❑ **Don't Remove Security Software or change settings**	On Tufts managed devices, security and other management tools are installed automatically. Do not change any security settings unless directed by TTS staff.
❑ **Tablets**	If you need or prefer to do official work on a Tablet other than accessing your Tufts calendar or email, you must use a TTS managed tablet.
❑ **Hard Disk Encryption on all Laptops**	All Tufts laptops are required to have full hard disk encryption.

	Most newer devices are already configured however if you don't meet the below conditions, contact the TTS Service Desk to check and get hard disk encryption enabled: • Windows devices received after February 1, 2020 should already have encryption configured using BitLocker. To check if BitLocker is enabled: go to Control Panel → System & Security → BitLocker Drive Encryption. It will say "C: BitLocker on" if BitLocker is enabled. • Prior to February 1, 2020, several groups had McAfee hard disk encryption installed. These groups typically were Advancement, HR, Friedman, and Dental. To check, you would either see the McAfee login screen upon reboot/power on or you will find it in the list of installed software on your device. • MACs since 2/1/2020 generally are encrypted.

3. Personally owned Laptops, Desktops, Tablets, Phones and Other Devices	
For personally owned equipment, you are responsible for installing and maintaining the technologies to the standards set forth in these Guidelines. Personally owned devices can be used to access public data and your Tufts email and calendar.	
❑ **Tufts Virtual Desktop – required with personal devices (with some exceptions)**	Central Administration and School Administrators must use Tufts owned devices that are managed centrally by TTS for accessing and performing Tufts work that involves institutional information except for data defined as public data or for only accessing your own personal information. When this is not possible other options include The *TTS virtual desktop service* or the *TTS laptop loaner program*. On an infrequent basis, personal devices may be used to connect to the TTS virtual desktop service so that your work can be performed remotely through the virtual desktop. In some cases using a TTS loaner laptop might be the best option. See TTS laptop loaner program.
❑ **Require a Password** for access to your device and **Use a Strong Password**	Use a strong, unique password to log into the device and protect your login/password by not sharing it with others (including family members). Follow the same requirements as for your Tufts password. Use a password manager. See Tufts Password.
❑ **Manually Lock your Screen or Power Off** when you leave your device	Every time you leave your device unattended, you should either turn it off or activate the screen lock that requires you to enter your password to resume working. See Screen Lock.
❑ **Set your Screensaver to Automatically Activate**	You should configure an automatic screen lock on your devices that requires you to enter a password to resume using the device after 10 minutes or less.
❑ **Review Privacy Settings**	Review the privacy settings on your devices and limit sharing to the minimum necessary. These settings limit applications' access to your location, contacts, calendars and reminders.
❑ **Apply Updates/Patches**	You are responsible for having all critical Operating System (OS), application, and browser security updates applied and kept up to date

	with all new security updates as they are released (for example, iOS, Apple, Microsoft, Adobe, Google, Firefox). Configure automatic updates wherever possible, and when patches are finished installing, follow any prompts to reboot the device to ensure proper functionality. • Windows updates and other protection tools and advice can be obtained at: http://www.catalog.update.microsoft.com/Home.aspx • Apple updates are available at: https://support.apple.com/en-us/HT201222 or via iTunes Be sure to also update your mobile devices routinely, including your smart phones or tablets. Updates can generally be found on the company website by searching for "security updates."
❑ **Install and use Antivirus Software**	All devices connected to Tufts via remote site access technologies must use current and updated antivirus software to assist in protection from hackers and malware. There are a number of options both free and for purchase. Faculty, staff and students may purchase a version of Trend Micro through the university at a discount. Go to https://access.tufts.edu/antivirus. There are many other vendors with inexpensive options such as McAfee or Norton and free options such as AVG, Malwarebytes, Avast, Sophos and Bitdefender. See Antivirus Applications. When downloading free software, use a trusted website, such as download.cnet.com.
❑ **Configure the Firewall & Privacy Settings**	All devices connected to Tufts remotely, including via wireless, should employ a software or hardware-based firewall. Most operating systems have built-in firewalls and enhanced security and privacy settings that can be turned on and configured. As an alternative, a firewall can generally be purchased and/or installed where you purchased your device.

4. Using ALL DEVICES: Laptops, Desktops, Tablets, Phones and other Devices whether Tufts Provided or Personally owned	
❑ **Only Install Trusted Applications**	Only install trusted applications from reputable software providers, such as download.cnet.com, Apple Store, Google Play, Microsoft.com
❑ **Protect your WiFi and Bluetooth Settings**	*Disable Mobile Hotspot:* Nearly all laptops, tablets, and phones have a feature to act as a Mobile Hotspot. Make sure that this feature is turned off on all your devices. When/if you need to use it, make sure to set a password and change it periodically then turn off the mobile hotspot when done. *Sharing between phones*: Phones and tablets make it easy to share files direct to a nearby device. Often this is enabled by default and can allow others to connect to your device without your permission. On your phone/tablet disable AirDrop (iPhone) or Nearyby Share (Android) until when/if you actually chose to use it. *Bluetooth Sharing/Pairing:* It's recommended that review your device's Bluetooth settings to make sure you are alerted when another

	device is trying to pair with yours. Also consider if you want to leave the Bluetooth as "discoverable" which will broadcast your device name to others searching for Bluetooth connections. **For help:** Go to the Microsoft, Apple, or similar support pages to find out more about how to find and change these settings on your device.
❑ **Limit Sharing of Devices**	Tufts-owned devices must not be shared with other persons outside of Tufts, including family members. If you share a personally owned device with family members, be sure to log out of all Tufts tools and information before permitting anyone else to use the device. Consider carefully whether to share a device that you also use for your Tufts work. Often it is through family members that malicious software is inadvertently downloaded to a device.
❑ **Physically Protect all Portable Devices**	Portable devices, such as phones, flash drives, external hard drives, laptops, and other mobile devices, are particularly vulnerable to theft. They are easily lost or misplaced. All portable devices must be kept secure, password protected and locked when unattended.
❑ **Do Not Allow Other Persons you do not Know and Trust to Connect to your Devices**	Seeking to connect to a device through deception (pretending to help clean up viruses or provide remote technical assistance) is a common ploy used by hackers. Do not permit any such connection. The only safe/permissible remote connection is by the TTS Service Desk that is initiated only after you have contacted them.

Access & Data Management

5. Accessing Tufts Services – Using the Home and Tufts Network	
❑ **Use the Tufts Virtual Private Network (VPN)**	When connecting to the Tufts internal network or data from off campus, some Tufts services may require you to use the **Tufts Virtual Private Network (VPN).** If it is not already installed, go to: Tufts VPN. This site has instructions on how you can download and use the VPN client software.
❑ **Use Two-Factor Authentication (2FA) and Beware of Unexpected Requests**	*Tufts 2FA:* For your protection and for Tufts, you have been required enroll and use Tufts Two Factor Authentication (2FA) to access many of Tufts' tools and services. It is based on a solution from Duo and this ensures many of Tufts' applications, including the VPN, can be locked down so that if your userID and password are stolen, you will be protected. More information is available at https://it.tufts.edu/qs-twofactor. *Unexpected Duo Prompt/Call*: If you receive an unexpected prompt for a Duo authorization, deny the push or hang up the phone. It is highly likely someone has stolen your UserID and password and is trying to log in as you. As soon as possible, call the 24x7 TTS Service desk at 617-627-3376, and tell them you got an unauthorized Duo request. You also need to change your password. *Personal Use of 2FA/MFA:* Most of your personal accounts, especially banks, offer the ability to use 2FA or Multi-Factor Authentication (MFA). Just about every type of online account is valuable to hackers

	so enable 2FA/MFA wherever you can. *HINT*: The Duo phone app can be used to authenticate to almost any 2FA or MFA service (even Google and Microsoft). When setting up the MFA, there is a step to connect it to a phone app. Usually there is a QR code to authorize and connect the app to the account. Open the Duo app, select "add account", and follow the instructions.
❑ **Securely Configure your Home/Off-site Wireless or Wired Network**	It is your responsibility to have a secure wired or wireless environment. *Wireless network:* To help reduce the risks associated with home wireless networks, use the following configurations: • Enable WPA2 encryption • Change the default SSID for your wireless router • Change the default Administrator Passwords and Usernames for your wireless router • Apply all routine patches or updates to the operating system or "Bios" of routers, wireless routers and switches *Wired network:* If you have a wired home network, make sure the default passwords to your routers and other network equipment have been changed and that it is routinely patched. *Wireless/Wired Networks:* Also, enable firewall protection for your network. You can either enable an imbedded firewall on your router (if available) or install a separate firewall device. Some example devices to consider for WiFi: Eero, Google Nest WiFi, Deco, Orbi, etc. or Wired: Bitdefender Box2, Firewalla Red/Blue, Netgear ProSAFE, etc.
❑ **On-campus WiFi networks**	Tufts has a WiFi network when working on one of Tufts campuses. When connecting, use the **Tufts-Secure** WiFi network. The others (Wireless, Guest, Other) have specific purposes that are rarely needed by most of the Tufts community. If you see that your device has connected to one of these other networks, go into network settings and do the equivalent of "forget this network". For performing Tufts duties, you should only use Tufts-Secure WiFi.
❑ Tufts Virtual Desktop when needed	Use this secure virtual computer service that allows users to perform Tufts work from a personal device or to use specialized software. It can be used without connecting to the Tufts VPN.
❑ **Access and Use Email Carefully**	Tufts non-public information (see definition in the Information Classification and Handling Policy) should never be sent from/sent to your personal email. *Web Access to Tufts email:* Tufts provides remote access to your Tufts email through the *Microsoft O365 Email-Outlook Web App* at https://outlook.office.com/ Use this application for email communications for your university-related work. *Using Personal device for Tufts email*: You can also sync your Tufts email to your personal device using the native email client on your device or by downloading the Outlook App to the device. The TTS website includes information about setting up email on your mobile phone, including selecting using a secure connection. See Office 365 Email Set Up. During this setup you will be prompted for some

	additional security settings to be configured if you have not already done so. If you sync your Tufts email to your personal device, it is *very important* that you understand that you will then have a copy of emails on your device. You must be sure to handle the email appropriately and securely control your device. Always be especially alert to your security practices if sensitive information is included in an email. See the discussion below under Data Management about what information may never be stored on a personal device, whether by syncing email or otherwise.

6. Data Management	
❑ **Understand Tufts Rights to Institutional Data regardless of location or device ownership**	Tufts retains its rights in its institutional data regardless of where it is stored or how it is accessed. Tufts may need to inspect a personally owned device that has accessed or maintained institutional data or may have violated copyright laws while using Tufts networks. Records or data maintained by employees and others affiliated with Tufts may be the subject of document requests under FERPA or other laws and regulations or document production requirements pursuant to warrants, subpoenas, court orders and other requirements. University employees are obligated to produce those records or data, or the devices on which they are stored, upon request of the University. To fulfill these requirements, Tufts data should be stored in Tufts Box or on Tufts network drives, rather than locally.
❑ **Know where Data is Stored and Store it only in Approved Locations**	Restricted or Confidential Institutional Data must never be stored on any personally owned device or in a personal email account. This includes sensitive personal information (SPI), and Personal Health Information (PHI) for covered entities under HIPAA. Definitions and examples can be found in the Information Classification and Handling Policy. The one permitted exception to storing information on a personal device is the syncing of your Tufts Outlook/O365 email to your personal device. You can use the native email client on the device or by downloading the Outlook App to the device. See the information above in section 5 "**Access and Use Email Carefully**". You should always store any file with Tufts Restricted or Confidential information on either in Tufts Box (if permitted by the Tufts Box Use Guideline), on a Tufts network drive, or another Tufts approved location. Any device could potentially be lost or stolen, leaving the data open to whomever takes your device. A device can be left on the subway, but a network drive or Box folder cannot. Do not use Box Sync to sync Tufts information to a personally owned device. Tufts information should not be stored in applications that have not

	been vetted for use at Tufts, such as DropBox, Survey Monkey, or your personal Google Drive. Unlike approved services like Tufts Box, Tufts OneDrive, and Tufts Google, Tufts has no agreement with these vendors for the protection of Tufts information.
❑ **Separate Personal and Institutional Information**	If any Tufts information is temporarily stored on a personally owned device, even if it is not sensitive information, always keep it separate from your personal information and files as much as possible and securely delete the Tufts information as soon as it is no longer needed.
❑ **Back-up your Data**	Devices can fail, lost, stolen, or be compromised by ransomware and other malware, and without a back-up, your files will be lost. The Tufts *best practice* is to protect your work by storing it in Tufts Box and using your computer to work with the files directly while stored in Box. See more information in the Box Use Guide. If you keep and work with your data only locally, you need to regularly make an electronic copy and store it safely in Tufts Box. Information stored in Tufts Box and on the university shared drives is regularly backed-up. If you only store information on your device, such as on the Desktop, an external USB device, or in Documents, the information will not be backed-up by a Tufts service. This is NOT a recommended. If you are unable/unwilling to use Tufts.box.com then you should sign up for the Tufts CrashPlan service. Note this will be an additional fee to your department. You are highly encouraged to switch to storing your data in Tufts.box.com
❑ **Access Only What is Needed**	Only access or maintain sensitive information when you have a need to know the information to perform your duties. The less you have, the less you have to protect and maintain.
❑ **Securely Delete or Return Data when No Longer Needed or Upon Request**	When your responsibilities, role or employment status changes, you complete a project, or are no longer an authorized user of Tufts data: You are obligated to immediately return or securely delete the related institutional data accessed or maintained on all devices and any related paper files. See Section 7 “Securely Erase” for deletion tips. You are also obligated to immediately return or delete institutional data accessed or maintained on all personally owned devices upon request of the University.
❑ **Securely destroy any Paper Documents when no Longer Needed or Upon Request**	To securely dispose of paper documents, either use a cross-cut shredder (micro-cut preferred), not a strip shredder, or bring the documents to Tufts and place them in a locked bin served by Shred-It, the Tufts approved vendor for secure removal and shredding.

7. Selling, Transferring, or Disposing of any Device: A Laptop, Desktop, Tablet, Printer, Copier, Scanner, Fax Machine, USB stick and External Hard Drives

❑ **Securely Erase all Devices when Your Use Ceases**	If you used any personally purchased or leased device – including a laptop, desktop, tablet, phone, USB stick, external hard drive, printer, scanner, copier, fax machine or other device - for your work with Tufts

	information, then before you sell, transfer, return, gift or dispose of the device, you must securely wipe the device. By doing so, you will protect the information retained on the hard disc or the device from disclosure to and use by persons who are not permitted to have the information. **Advice on how to securely erase data:** • For Windows computers click HERE or search Microsoft Support HERE • For Apple devices, go to Apple Support and search "secure erase" for your device. Click HERE • For Tufts devices: contact the TTS Service Desk at (617) 627-3376
❑ **Return any Tufts owned Device when Your Use Ceases or Employment Ends**	If a laptop, desktop or other device was purchased by Tufts, you must return it when your employment ends, when it is no longer being used, or has reached end of support, unless otherwise agreed in writing with an authorized Tufts representative. When it is returned to Tufts, it should always be sent to TTS to have the hard drive securely wiped. Devices that have reached end of support should NOT be passed on to others or stored for some potential future use. Contact the TTS Service Desk at (617) 627-3376 for advice on how and where to return the device. If you have been granted permission to retain the device, the hard drive must first be securely wiped by TTS to remove Tufts institutional data.

Reporting Incidents with Security Implications

8. Reporting Lost Devices and other Security Incidents	
❑ **Report a Lost Device or any other Security Incident Immediately**	If you have lost or had stolen a laptop or other device, suspect there has been an unauthorized disclosure of information, or are concerned another information security incident has occurred – whether involving a Tufts managed device or a personally owned device – immediately contact the Service Desk and follow the steps provided at Reporting Information Security Incidents. If the device was stolen, also report the theft to the TUPD at (617) 627-3030 or the local police.