Tufts Technology Services (TTS)
Technology Guidelines and Services for Working Off-Campus, Telecommuting, and Personal Devices

Purpose and Scope
These Guidelines describe actions you can take to protect Tufts information and resources when working outside the Tufts on-campus computing and network infrastructure and when using personal devices. By reviewing these Guidelines, you will become familiar with industry best practices and the University's expectations when using or accessing computing resources and/or Tufts data from "off-campus" and when using personal devices.

These Guidelines include expectations for the use of both Tufts provided and managed devices and personally-owned devices when working off-campus and for the use of personally-owned devices when working on-campus or off-campus. However, these Guidelines do not specifically address expectations when travelling, whether domestically or internationally, or when working remotely from outside the United States.

Overview of Technology Guidelines

1. Tufts Provided and Managed Laptops and Desktops
2. Personally-Owned Laptops, Desktops, Tablets, Phones and Other Devices
3. ALL DEVICES: Laptops, Desktops, Tablets, Phones and other Devices whether Tufts Provided or Personally-Owned
4. Accessing Tufts Services - Using the Tufts Network
5. Data Management
6. Selling, Transferring or Disposing of any Device: A Laptop, Desktop, Tablet, Printer, Copier, Scanner, Fax Machine, USB stick, and External Hard Drives
7. Reporting Lost Devices and other Security Incidents

Your Responsibilities
When working remotely with Tufts information or resources or when using a personally-owned device, you are responsible for your working environment. 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.

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 working remotely and/or using personally-owned devices.

You are expected to routinely monitor university communications on policy changes and comply with changes in all applicable policies and guidelines.

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

TTS Services

Services for Working Off-Campus	
The TTS website at it.tufts.edu provides links to access Tufts' full range of technology services and includes practical guides to how to use them.	
❑ Tufts VPN	Use a secure and private connection to the Tufts network from off-campus
❑ Jabber	Make calls by VoIP and chat (instant messaging) using any computer or mobile device
❑ WebEx	Host and attend audio and video conferences, presentations, and meetings
❑ Outlook Web App: exchange.tufts.edu	Access email, calendar and other Exchange services
❑ 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, access, and share content securely. See Tufts Box Use Guideline for permitted uses and Box Use Guide.
❑ Service Desk Remote Assistance	Enables access to your computer remotely to resolve problems
❑ Access Tufts	Access everyday administrative tasks in one place

Technology Guidelines

1. Tufts Provided and Managed Laptops and Desktops	
In the case of Tufts provided and managed equipment, many of these guidelines are part of the standard TTS configuration when a laptop or desktop is deployed, as noted by a "*****". Having your device managed by Tufts significantly reduces your device management 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. If the Tufts managed device is not being properly maintained, you are responsible to work with Tufts to resolve the issues. **If you are uncertain if your Tufts provided device is Tufts managed, contact the TTS Service Desk.**	
❑ **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 or less. If your Tufts device is not so configured, 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 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 Antivirus Software and Firewall***	On Tufts managed devices, antivirus software and a firewall are installed automatically. If they are missing or not working, contact the TTS Service Desk.
❑ **Register Device and Install LANDesk***	In order for any Tufts provided devices to be managed properly and to facilitate assistance with any issues, all Tufts-owned devices must be registered and have LANDesk installed. If you have any questions regarding device registration and LANDesk, contact the TTS Service Desk.
❑ **If using Restricted Information, enable Encryption on all Portable Devices**	Laptops and other portable devices may **not** be used to store Sensitive Personal Information (SPI), Personal Health Information (PHI) for covered entities under HIPAA, any other data subject to a regulation, and any other Restricted Institutional Data, unless the device is both (1) Tufts provided and managed, and (2) whole disc encrypted. *Restricted Institutional Data* includes data for which the unauthorized disclosure or unauthorized use may have a severe adverse effect on the university's reputation, finances, or operations, or on individuals. This classification includes data governed by privacy or information protection requirements articulated by law, regulation, contract, binding agreement, or industry groups. For other sensitive information, it is *highly recommended* that any laptop or other portable device used to store the information be whole disc encrypted. To have a Tufts owned laptop whole disc encrypted, contact the TTS Service Desk.
2. 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.	
❑ **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, 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: http://support.apple.com/kb/HT1222 or via iTunes Be sure to also update your mobile devices, 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.
❑ **Install a Firewall**	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 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.
3. 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.
❑ **Use Secure WiFi and Bluetooth Settings**	It's recommended that you turn off optional network connections, such as for WiFi and Bluetooth, when you are not using them. Also, limit your WiFi sharing settings to the minimum needed. Be aware that Wi-Fi Sense, which is part of Windows 10, versions earlier than 1803, may share access to your networks with others and connect you to open networks automatically. Update your Windows 10 version.
❑ **Limit Sharing of Devices**	Tufts-owned devices should 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

	any one 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 is a common ploy used by hackers. Do not permit any such connection. The only permissible remote connection is by the TTS Service Desk, after you have contacted them.
4. Accessing Tufts Services - Using the Tufts Network	
❑ **Use the Tufts Virtual Private Network (VPN)**	When connecting to the Tufts internal network or data from off campus, you should **always first connect to the Tufts Virtual Private Network (VPN).** The VPN provides an encrypted connection to access all Tufts' network shares as well as any Tufts site or application that has sensitive data. Go to: Tufts VPN. Once connected, there are instructions on how you can download and use the VPN client software.
❑ **Enroll in Two-Factor Authentication**	For your protection, you are required enroll to use Tufts Two Factor Authentication to access many of Tufts' tools and services. It is based on a solution from Duo. When you enroll in this solution, many of Tufts' applications and the VPN can be locked down so that if your userID and password are stolen, you will be protected. Logging in to Tufts using Duo requires two steps: first entering your userID/password, and then second, requesting verification through Duo. More information is available at https://it.tufts.edu/qs-twofactor.
❑ **Securely Configure your Home/Off-site Wireless or Wired Network**	It is your responsibility to have a secure wired or wireless environment. 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
❑ **Use Email Carefully**	Tufts non-public information should never be included in any personal email. For employees, Tufts provides remote access to your Tufts email through the *Microsoft Exchange Email-Outlook Web App* at exchange.tufts.edu. Use this application for email communications for your university-related work. For students, Tufts provides email via Microsoft Office 365, with access through https://login.microsoft.com/ . Employees can also sync their exchange email to their personal device using the native email client on their device or by downloading the Outlook Exchange App to the device. If you sync your 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. The TTS website includes information about setting up email on your mobile phone, including selecting using a secure connection. See Exchange Email Set Up. See the discussion below under Data Management about what information may never be stored on a personal device, whether by syncing email or otherwise.
5. Data Management	
❑ **Understand Tufts Rights to Institutional Data when located Off-Campus**	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 Institutional Data may *never* be stored on any personally-owned device. This includes sensitive personal information (SPI), and Personal Health Information (PHI) for covered entities under HIPAA. ***Restricted Institutional Data*** includes data for which the unauthorized disclosure or unauthorized use may have a severe adverse effect on the university's reputation, finances, or operations, or on individuals. This classification includes data governed by privacy or information protection requirements articulated by law, regulation, contract, binding agreement, or industry groups. Examples can be found in the Information Classification and Handling Policy. Also, you should not store any Tufts ***Confidential*** information on a personally-owned device. At Tufts, all institutional data is Confidential Institutional Data unless the data has been designated as or otherwise qualifies as either Restricted Institutional Data or Public Institutional Data. Confidential Institutional Data includes data for which unauthorized disclosure or use may have a significant adverse effect on the university's reputation, finances, or operations, or on individuals. Examples can be found in the Information Classification and Handling Policy.

	You should always store any file with Tufts Restricted or Confidential information on either a Tufts network drive, in Tufts Box (if permitted by the Tufts Box Use Guideline), 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. The one permitted exception to storing information on a personal device is the syncing of your exchange email to your personal device using the native email client on the device or by downloading the Outlook Exchange App to the device. See the information above under Email. 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 Google Docs, Google drives, DropBox, and Survey Monkey. Unlike approved services, 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 or be compromised by ransomware and other malware, and without a back-up, your files will be lost. Protect your work by regularly making an electronic copy and storing it safely. Information stored in Tufts Box and on the university shared drives is regularly backed-up. However, if you only store information on a device, such as on the Desktop, an external USB device, or in Documents, the information will not be backed-up by a Tufts service.
❑ **Access Only What is Needed**	Only access or maintain sensitive information when you have a need to know the information to perform your duties.
❑ **Securely Delete or Return Data when No Longer Needed or Upon Request**	When your responsibilities, role or employment status changes or you complete a project such that you no longer require institutional data you have accessed or maintained on a personally-owned device or are no longer an authorized user of that data, you are obligated to immediately return or securely delete the institutional data accessed or maintained on all personally-owned devices. 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.
6. 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.
❑ **Return any Tufts owned Device when Your Employment Ends**	If a laptop, desktop or other device was purchased by Tufts, you must return it when your employment ends, 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. If you have been granted permission to retain the device, the hard drive should first be securely wiped by TTS to remove Tufts institutional data.
7. 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 police.