

RESTRICTED INSTITUTIONAL DATA HANDLING GUIDELINES



Making confidentiality and privacy part of your daily work

Follow These 10 Key Strategies

- 1** *Focus on what Information is Needed*
 - Collect only what you need
 - View only what you need
 - Keep only what you need
 - Share only what is needed
- 2** *Only use Secure Devices*
 - Encrypt laptops and other portable devices
 - Don't use any Tufts device for Restricted Information unless it is managed by TTS or follows TTS standards
 - Do not store Restricted Information on personal devices (see special rule for Tufts email)
- 3** *Protect Information on your Devices*
 - Keep it Private. Lock devices when not in use and block from view. (Lock and Block)
 - Back up the information on your devices
 - Update (patch) your software. Use antivirus software.
- 4** *Use Secure Tufts Approved Apps and Tools*
 - Only use apps and tools approved for Restricted Information.
 - Box approved for all Restricted Data other than credit card data or some research data
 - Don't use DropBox or Google tools for Restricted Information
- 5** *Restrict your Use of Email*
 - Only use 1 of 3 encrypted options:
 1. Stay within the @tufts.edu email system
 2. For outside of Tufts, use Tufts [Secure] email
 3. For within Tufts or outside Tufts, send an encrypted attachment and use a password sent separately
 - Never use personal email for Restricted Information
- 6** *Use Tufts_Secure for campus wireless. Use the Tufts VPN to connect to Tufts services when off campus.*
- 7** *Print and Scan with Care*
 - Only use approved copiers, printers, scanners and fax machines kept in a secure place.
 - Have wiped before disposing of the machine.
- 8** *Protect your Paper Documents*
 - Use two locks for paper documents. Shred with cross-cut shredder or Shred-It bins.
- 9** *Be Prepared for Rights Requests*
- 10** *Immediately Report a Security Incident to the TTS Support Desk*
Call by phone at: 617 627-3376. Also see [Reporting an Information Security Incident.](#)

Important Note:

Even if you don't use Restricted Information frequently in your work, you probably handle other types of sensitive, confidential information in your work. It's important that everyone learn good handling practices for all University information. You can use the same handling practices you'll learn in these Guidelines when you work with any sensitive information at Tufts.

I.	WHAT IS RESTRICTED INSTITUTIONAL DATA	1
1.	Definition of Restricted Institutional Data (also known as Restricted Information)	1
2.	Categories and Examples of Information included in Restricted Institutional Data	1
A.	Information Protected by a Law, Regulation or a Requirement of an Industry Group	1
B.	Information Protected under an Agreement.....	2
C.	Other Restricted Information	2
II.	WHY IT IS IMPORTANT TO PROTECT RESTRICTED INFORMATION	2
III.	KEY STRATEGIES FOR RESTRICTED INFORMATION	3
1.	Focus on What Information is Needed.....	4
A.	Collect only what you Need – How to Collect Restricted Information	4
B.	View only What you Need	5
C.	Share only What is Needed	5
D.	Keep only What you Need – When and How to Store Restricted Information	7
2.	Only use Secure Devices	10
A.	Tufts Laptops and Tablets - Encryption is Required	10
B.	Tufts Desktops, Laptops and Tablets	11
C.	Restrictions on using your Personal Devices	11
D.	Smartphones and Tufts Email.....	11
E.	Public Computers.....	12
F.	USBs, Discs, and similar Portable Devices and Media	12
3.	Protect Information on your Devices.....	12
A.	Keep it Private.....	12
B.	Back up your devices.	13
C.	Update (Patch) your software. Use antivirus software.	14
4.	Use Secure, Tufts Approved Apps and Tools	14
A.	Apps, Tools and Services from Third Party Vendors and Service Providers	14
B.	Stopping Using an Outside Service or Vendor	15
C.	Passwords	15
D.	Two Factor Authentication	16
5.	Restrict your use of email. Follow the Five: How - Who - With - What - Done	16
A.	How to send a Restricted Information Email: Use @tufts.edu and Encryption	16
B.	Limit Who will be able to Read your Email Message.....	19
C.	Consider sending the Email With a Special Notice or Flag	20
D.	Limit What is included in the Email	20
E.	Securely Delete the Email to be Done	20
F.	Using Tufts Email on your Personal Smartphone, Tablet and other Devices	20
G.	Accessing your Tufts Email Off Campus on your Tufts Device	21
6.	Use Tufts_Secure WiFi and the Tufts VPN	21
A.	WiFi.....	21
B.	Virtual Private Network Connection for Working Off-Campus.....	21
7.	Print and Scan with Care	21
A.	All Copiers, Printers, Scanners and Fax Machines	21
B.	Special Rules for Sending Restricted Information Using Fax.....	22
8.	Protect your Paper Documents	22
A.	Keep Offices Physically Secure.....	22
B.	Protect Paper Documents when Working with Them	22
C.	Use Two Locks for Paper Documents.  	22
D.	Shred Securely	22

9.	Be prepared for rights requests	23
A.	Student Requests under FERPA	23
B.	Requests under the European Union’s (EU) General Data Protection Regulation (GDPR).....	23
10.	Immediately report any potential security incidents	23
IV.	SPECIAL RULES FOR SENSITIVE PERSONAL INFORMATION (SPI)	24
1.	Social Security Numbers	24
A.	Special Uses	24
B.	Last Four Digits	24
C.	Use of Social Security Numbers as Student ID Numbers	25
2.	Local Office and Departmental Policies	25
3.	Only Use Apps and Tools approved for use with SPI	25
4.	Incident Reporting	25
A.	Reporting Period; Affected Persons	25
B.	Reporting of Persons Involved.....	25
V.	ADDITIONAL REQUIREMENTS FOR EEA PERSONAL DATA PROTECTED BY THE GENERAL DATA PROTECTION REGULATION (GDPR)	26
1.	Know when your work requires complying with the GDPR	26
A.	GDPR and Collecting Personal Data when a Person is in the EEA	26
B.	GDPR and Established Programs in the EEA	26
C.	GDPR and Collecting Personal Data When Monitoring a Person’s Behavior	26
D.	The GDPR and Conferences	26
E.	The GDPR and Research	26
F.	The GDPR and Mailing Lists	27
G.	What is EEA Personal Data?.....	27
H.	What is “processing” under the GDPR?.....	27
2.	Minimize collecting, using and sharing EEA Personal Data	27
A.	Limit EEA Personal Data	27
B.	Anonymize and Pseudonymize	27
C.	Develop and Follow a Data Retention Plan	28
3.	Have a permitted Justification under the GDPR for processing Information	28
A.	Working with Personal Data is Necessary for a Legitimate Interest of the University	28
B.	Working with EEA Personal Data is Necessary in Connection with a Contract	29
C.	The Individual has Fully Consented to Tufts’ Processing their Information	29
4.	Give a Disclosure Notice	29
5.	Follow Stricter Requirements before Collecting or Using Special Category Information. 29	
6.	Only Use Apps and Tools approved for use with EEA Personal Data	30
7.	Have Written Agreements with Third Parties with whom you Share Personal Data	30
8.	Follow the requirements for transferring EEA Personal Data from the EEA to the US. ...	31
9.	Know the GDPR Rights for Individuals. Immediately Report Rights Requests.	31
A.	The GDPR Rights Individuals may Exercise	31
B.	Submitting a Rights Request.....	32
10.	Immediately report any potential Security Incident involving EEA Personal Data or other Restricted Institutional Data to the TTS Service Desk	32
VI.	SPECIAL SITUATIONS	33

1.	What to do if you receive Restricted Information that you did not request	33
2.	Working off campus and telecommuting	33
3.	Employees leaving your Office	33
VII.	HOW DO YOU GET HELP?.....	34
1.	Information Stewards	34
2.	TTS Website	34
3.	TTS Support Desk.....	34
4.	GDPR Consultations	34
	Appendix A: European Economic Area (EEA) Countries.....	35
	Appendix B: Required Strong Controls for Personal Devices.....	36

I. WHAT IS RESTRICTED INSTITUTIONAL DATA

1. Definition of Restricted Institutional Data (also known as Restricted Information)

Restricted Institutional Data is the information that should be handled with the University's highest level of confidentiality.

Under the University's [Information Classification and Handling Policy](#), Restricted Institutional Data is:

“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.”

In these Guidelines, we often refer to Restricted Institutional Data as *Restricted Information*.

2. Categories and Examples of Information included in Restricted Institutional Data

A. Information Protected by a Law, Regulation or a Requirement of an Industry Group

Examples in this category include:

- **Sensitive Personal Information (SPI)** protected by Massachusetts and other state privacy laws, as well as Tufts' policy, including:
 - Social Security numbers
 - Any other government issued numbers used for identification
 - Individuals' financial account numbers, including bank account numbers and JumboCash account numbers
 - Biometric indicators for identity (such as fingerprints)
- **Students' FERPA Data:** Students' Personally Identifiable Information in their Student Education Records (Federal Education Rights and Privacy Act (FERPA)) unless the information is Directory Information (as defined in the applicable University FERPA policy) for a student that has not requested a Privacy Block
- **Financial Aid and other Financial Customer Nonpublic Personal Information** subject to the Gramm-Leach-Bliley Act (GLBA)
- **Cardholder data collected from persons and entities paying Tufts,** subject to the Credit Card or Payment Card Industry Data Security Standards (PCI DSS)
- **HIPAA Protected Health Information (PHI)** protected by the Health Insurance Portability and Accountability Act (HIPAA)

- **Identifiable Human Subject research data**, including research data involving human subjects that are subject to the Common Rule (Federal Policy for the Protection of Human Subjects, 45 CFR 46.101 et seq)
- **Export controlled research** regulated by the International Traffic in Arms Regulation (ITAR) and Export Administration Regulations (EAR)
- **European Economic Area (EEA) Personal Data** of applicants, students, staff, faculty, research subjects and others protected by the General Data Protection Regulation (GDPR)
- **Federal Information Security Management Act (FISMA) data**

B. Information Protected under an Agreement

Examples include:

- Data sets provided to the University subject to a data sharing agreement requiring confidential handling
- Data collected in connection with a grant agreement or a data management agreement or plan
- Data protected by a Nondisclosure Agreement or a Confidentiality Agreement

C. Other Restricted Information

Examples include:

- Authentication data: passwords, keys, other electronic tokens
- Attorney Client Privileged information
- Information that has been classified by the Data Authority for that type of data as Restricted Institutional Data

II. WHY IT IS IMPORTANT TO PROTECT RESTRICTED INFORMATION

As Tufts employees and members of the Tufts community, we are all responsible for doing our part to be good stewards of the University's Restricted Information.

Here are some important reasons to protect Restricted Information:

- When you safeguard Tufts' Restricted Information, you help support and advance Tufts' mission.
- By protecting Restricted Information, you protect the University from fraud.
- When you protect persons' individual information, you help shield yourself, your colleagues, our students and other members of our community from identity theft and other fraud.
- When you follow the rules for handling Restricted Information, you support Tufts' obligation to comply with the laws and regulations that apply to the University.
- A violation of the rules and regulations that apply to Restricted Information could result in substantial fines, penalties and other costs., as well as damage to the A failure to protect Restricted Information in the manner we are required to could damage the University's reputation.

III. KEY STRATEGIES FOR RESTRICTED INFORMATION

Follow These 10 Key Strategies

- ① *Focus on what Information is Needed*
 - Collect only what you need
 - View only what you need
 - Keep only what you need
 - Share only what is needed
- ② *Only use Secure Devices*
 - Encrypt laptops and other portable devices
 - Don't use any Tufts device for Restricted Information unless it is managed by TTS or follows TTS standards
 - Do not store Restricted Information on personal devices (see special rule for Tufts email)
- ③ *Protect Information on your Devices*
 - Keep it Private. Lock devices when not in use and block from view. (Lock and Block)
 - Back up the information on your devices
 - Update (patch) your software. Use antivirus software.
- ④ *Use Secure Tufts Approved Apps and Tools*
 - Only use apps and tools approved for Restricted Information.
 - Box approved for all Restricted Data other than credit card data or some research data
 - Don't use DropBox or Google tools for Restricted Information
- ⑤ *Restrict your Use of Email*
 - Only use 1 of 3 encrypted options:
 1. Stay within the @tufts.edu email system
 2. For outside of Tufts, use Tufts [Secure] email
 3. For within Tufts or outside Tufts, send an encrypted attachment and use a password sent separately
 - Never use personal email for Restricted Information
- ⑥ *Use Tufts_Secure for campus wireless. Use the Tufts VPN to connect to Tufts services when off campus.*
- ⑦ *Print and Scan with Care*
 - Only use approved copiers, printers, scanners and fax machines kept in a secure place.
 - Have wiped before disposing of the machine.
- ⑧ *Protect your Paper Documents*

Use two locks for paper documents. Shred with cross-cut shredder or Shred-It bins.
- ⑨ *Be Prepared for Rights Requests*
- ⑩ *Immediately Report a Security Incident to the TTS Support Desk*

Call by phone at: 617 627-3376
See [Reporting an Information Security Incident](#).

1. Focus on What Information is Needed

Important Rules:

Only collect, use, handle, or store Restricted Information if it is necessary for your job responsibilities.

Do not request access to Restricted Information if it is not necessary for your job responsibilities.

Do not grant access to Restricted Information if it is not necessary for the person's job responsibilities.

Delete access to Restricted Information when it is no longer necessary for completing job responsibilities.

A. Collect only what you Need – How to Collect Restricted Information

Before you collect Restricted information, ask yourself whether you will need each of the kinds of information you plan to collect for a particular task. When it comes to Restricted Information, it is not enough to collect information because there is a chance it might be helpful in the future. More is not better.

1) Permitted Ways to Collect Restricted Information

Use these methods for collecting Restricted Information (except for credit or debit card data):

- ✓ Talk in person
- ✓ Talk on the phone
- ✓ Use US Mail, UPS, or FED Ex
- ✓ Use Tufts Interoffice mail
- ✓ Share a Box folder
- ✓ Share a Q, M, R or other Tufts shared network drive
- ✓ Use email, but be sure to follow the special rules included in the Email section below. For example, send the information so that it is encrypted.

2) A Special Note about Credit and Debit Card Data

The credit card industry imposes very specific rules on how we may handle credit and debit card information when Tufts is being paid by credit or debit card. The rules are called the Payment Card Industry Data Security Standards (PCI DSS). At Tufts, we segregate what systems are used for this type of information.

No school, department, center, employee, or any other person at Tufts is permitted to process internet-based payment transactions, credit or debit card payments or electronic funds transfers without approval and training from Treasury Operations. Contact the Treasury Department, Merchant Services ([Treasury Contact List](#)), which oversees compliance with PCI DSS, for more information.

3) Prohibited Ways to Collect Restricted Information

Do *not* use these methods to collect Restricted Information:

- ✘ Text messaging
- ✘ Your voicemail, unless you've changed the settings so that it doesn't go to email (Ask Support Desk for assistance.)
- ✘ Sending an email without following the special rules
- ✘ Using a cloud-service or other application that isn't approved by Tufts Technology Services for Restricted Information (for example, DropBox and Google Drive are not approved)
- ✘ Writing it down on a post-it note and leaving it on your desk

4) How to Use Box to Collect Restricted Information

1. Create a new Box folder
2. Share that folder only with the person that needs to give you Restricted Information
3. Using Box, invite the person to the folder
4. Ask the person to upload the document with the Restricted Information to the shared folder
5. Move the document to a private Box folder not shared with the person, and permanently delete the document from the shared folder

5) Using Forms You Request Others to Complete

- ✓ State on the form how the form should be returned. Unless the form is using an online tool that has been approved to be used for Restricted Information, tell the users to return the form by mail or a similar service or deliver it in person. Email should not be used unless the form is being emailed *only* from a @tufts.edu to an @tufts.edu address. See the section on email.
- ✓ Handle and store any completed form that contains Restricted Information in accordance with the guidelines for storing.

B. View only What you Need

Important Rule:

Looking up personal information about an individual student, faculty, staff member or any other person out of curiosity, even if you don't intend to use or share the information in any way, is always prohibited.

C. Share only What is Needed

Only share information with others, whether in your office or with another office, if they need the information to do their work. For example, take the time to delete unnecessary information from a spreadsheet when only some of the information is needed. Be very careful about providing another department a

Social Security number. If you're not sure why the other department may need the Restricted information, it's good practice to ask.

If you receive a request for Restricted Information, refer the call or request to a staff member who has responsibility for that type of information and who is knowledgeable in the regulatory requirements that apply to that information.

Be careful not to share information by accident. Don't discuss sensitive information outside the workplace or with anyone who doesn't have a *need to know*.

Stay aware that other people can often overhear what you say. For example, don't repeat ID numbers when you collect them on the phone if others can overhear you. Be careful to protect a student's information during office conversations.

1) Permitted Ways to Send Restricted Information (except credit and debit card data)

- ✓ Talk in person
- ✓ Talk on the phone
- ✓ Use US Mail, UPS, or FED Ex
- ✓ Use Tufts Interoffice mail
- ✓ Share a Box folder
- ✓ Share a folder in the Q or other Tufts shared network drive
- ✓ Use email, but be sure to follow the special rules included in the Email section below. For example, send the information so that it is encrypted.

2) Prohibited Ways to Send or Provide Restricted Information

- ✗ Text messaging
- ✗ Using voicemail (you won't know whether it'll be translated into the recipient's email)
- ✗ Email without following the special rules
- ✗ Using a cloud-service or other application that isn't approved by Tufts for Restricted Information (for example, DropBox and Google Drive are not approved)

3) WebEx for Restricted Information

When your WebEx session will include Restricted Information, follow these steps to protect the confidentiality and privacy of the information:

- Schedule the meeting so that participants are not allowed to join before the host.
- Request that meeting invitations are not shared or forwarded. Limit sharing privileges to a small number of people.
- Ask unidentified call-in users to identify themselves before continuing the meeting.
- Monitor the list of participants to track who is joining the meeting.
- Be mindful that when you share your screen through WebEx, your entire screen will be visible to all participants. Be sure to close any

document that contains Restricted Information if it is not intended to be shared.

- If you record the meeting in WebEx, set a password on the recording, remove the recording from WebEx immediately, and store it outside of WebEx in a Tufts Box folder.
- Consider assigning a password to the call. Do not re-use passwords and do not use personal or common passwords. Don't include the password in the meeting invitation. Communicate the password separately or use a formula to construct the password that the person can use based on information they know (combination of facts/numbers).

4) Control Access to Files

- *Pay close attention to who has access.* Always limit access to records containing Restricted Information to those persons who need to know the Restricted Information for their job responsibilities.
- *Review folder access.* Schedule regular reviews of who has access to folders with Restricted Information. Remove access for anyone who no longer needs access, including anyone who has left your office, even if they are still at Tufts.
- *Not sure who has access to a folder in a network drive?* It can be hard to know who has access to a folder in a network drive. If you aren't completely sure who has access, put in a ticket to the TTS Support Desk.
- *Controlling Access in Box.* Box makes it easy to see who has access to a folder and to change who has access. The TTS website at [Box Data Storage and Collaboration/ Sharing Files and Folders](#) and at [Box Security Tips](#) has step-by-step directions on how to:
 - Set up access to folders (use the permission level with the least rights necessary)
 - Change access to folders
 - Choose the right settings to limit access
 - Safely share links (Use Invited People Only)
- Do not grant access to Tufts Box folders that contain Restricted Institutional Data to non-Tufts persons, unless a person with authority to do so has signed an authorization permitting the access.

D. Keep only What you Need – When and How to Store Restricted Information

After you have finished working with Restricted Information, before you store a copy in a file cabinet or electronically, ask yourself these questions:

- Will I need to use this information again?
- Is there an office that is responsible for managing this information so that if I need a copy later I can get it from them?
- Is my office required to keep this information? What is my office's policy? What is the University's policy?
- Are these records part of - or am I aware they could be part of - a legal action or proceeding, litigation, audit, investigation, or review?

- If I am keeping a copy, does my office have a practice of removing the information when it is no longer needed? How long should this information be kept based on the University's records schedule?

Always limit the length of time that you store records containing Restricted Information to the time reasonably necessary to accomplish a legitimate business purpose or to comply with governmental regulations. See the general [Records Retention Schedule](#) to learn how long offices and departments need to keep their records and what they should ultimately do with their records.

The head of each business unit or department, working with Digital Collections and Archives (DCA), is required to define retention periods for records with Restricted Information in accordance with University policies and procedures. Liz (Elizabeth) Francis, the University Records Manager, based in the DCA, consults with staff about record management.

1) Storing Paper Documents - Use 2 Locks

1. Use a locked file cabinet or desk drawer
2. That is in a locked office, room or other space

Secure the keys

- ✓ Limit access to employees who need the locked information
- ✓ Consider using a lock box with a combination code for the keys
- ✓ Change the code or where the keys are kept whenever an employee who had access stops working in your office

2) Storing Electronic Documents

Using designated departmental shares such as folders on the Q, M or R drives is permitted, except for credit and debit card information for payments made to Tufts.

Box is approved for storing Restricted Information, except for credit and debit card information for payments made to Tufts and some research data. See the [Tufts Box Use Guideline](#) for more information on what may be stored in Tufts Box. Also see [Box Security Tips](#).

Follow the access information above under Control Access to Files.

3) Prohibited Cloud Services (Services that Store Information on Non-Tufts Servers)

Do NOT use any unapproved cloud service, such as DropBox or Google Drive, to share or store any document that includes Restricted Information. If you are uncertain whether a tool or service includes a cloud service, contact the TTS Support Desk.

4) Servers in your Office

Important Notice:

In most cases, TTS does not manage servers located outside the University's data centers on a regular, ongoing basis. If your office has a local server that stores Restricted Information, contact the TTS Support Desk to determine whether special arrangements have been made to have TTS manage the server. If those arrangements have not been made, then your office is fully responsible for using appropriate practices to securely protect all Restricted Information, as well as other University information, stored on the server. To request assistance from TTS, contact the TTS Support Desk.

5) Do not Store Restricted Information in Email

For security reasons, NEVER use email to store Restricted Information, except temporarily.

Also, if important information is stored in email, it may not be available to persons who need to collaborate with you or who need to take on your work after you leave your position. In most cases, email accounts expire shortly after an employee leaves Tufts and the content may cease to be available.

6) Deleting Electronic Documents with Restricted Information

Be sure to securely dispose of the document or email on all devices and in all locations. Search for other copies of the document saved elsewhere.

Documents on a PC: delete the document and empty the trash/recycle bin.

Documents on a MAC: Use Empty Trash. Right click on the Trash can, select Empty Trash, and in pop-up, select Empty Trash.

Emails: To securely delete email messages and their attachments, see the three steps in [Securely Deleting Email](#). After deleting the message and emptying the Trash, you also need to purge the email to fully delete it.

For Tufts Box: Place in Trash, and then open Trash and Delete so the document is not recoverable. Otherwise, the document will be recoverable for 30 days. Be especially careful to locate all folders having copies of the document. See [Deleting and Restoring Content in Box](#).

7) Removing or Redacting Information in Electronic Documents without Deleting Document

First, delete the information in the document, and then delete all prior versions.

In Box, save as a new document, and delete the old document to protect against recovery of prior versions.

For Adobe pdfs: Use Adobe Secure to redact.

8) Disposing of Paper Documents - Shred to Destroy

Use one of the following:

- A micro-cut (preferred) or cross-cut shredder that cuts into squares or rectangles. Don't use a shredder that cuts in strips like linguine; or
- Secure disposal bins from Shred-it, the only Tufts approved vendor. Keep the bins in a secure location.

9) Removing or Redacting Information from Paper Documents

Use one of the following:

- Use opaque (100% impenetrable by light; neither transparent nor translucent) tape or paper to cover over the sections to be redacted. Do not use plain paper as the scanner may pick up images through the paper. Even some black paper may allow some light reflection - so be careful. Copy after redacted and shred or otherwise properly dispose of the original. Confirm that the redacted area of the copy is completely opaque.
- Cut-out (literally) all the text to be redacted and properly dispose of the clippings (i.e. shred). This method will always be 100% effective.
- Do NOT black out information using ink. It can still be recovered using tools like Photo-Shop.

2. Only use Secure Devices

A. Tufts Laptops and Tablets - Encryption is Required

Important Rule:

All Restricted Institutional Data stored on a portable device, including, without limitation, laptops, tablets, mobile phones, external hard drives, usb sticks and other media to store data, must be encrypted.

Contact the TTS Support Desk for encryption information and full-disk encryption services for Tufts-owned devices.

B. Tufts Desktops, Laptops and Tablets

You may use Tufts supplied and managed desktops, laptops and tablets for Restricted Information. Save the data on the desktop, laptops and tablets only as provided in these Guidelines.

Important Rule:

A desktop, laptop or tablet that is owned or provided by Tufts, but is *not* managed by TTS, may *only* be used for Restricted Information if:

- the desktop, laptop or tablet is protected by the Required Strong Controls in Appendix B, and
- it uses a secure connection, such as the Tufts VPN or Tufts_Secure.

To find out if your Tufts desktop, laptop or tablet is managed by TTS, contact the TTS Support Desk.

C. Restrictions on using your Personal Devices

Important Rule:

Tufts restricts using your home or other personal desktop, laptop, smartphone or other device for working with Restricted Information. You may *not* use your personal devices for Restricted Information, unless you use all of the following security protections:

- the device is protected by the Required Strong Controls (listed in Appendix B)
- the device is used *only to view* Restricted Information (rather than have the information downloaded onto it or stored on it), and
- it uses a secure connection, such as the Tufts VPN or Tufts_Secure.

A personal device may **never** be used to store Restricted Information, whether in “Documents,” the “Desktop,” “Downloads,” “Notes” or another location, except temporarily for email on a protected smartphone, which is discussed in the next section.

Users are encouraged to use a Tufts provisioned Virtual Desktop Interface (VDI) via the Tufts VPN to access Restricted Institutional Data when using personal devices.

D. Smartphones and Tufts Email

There is one permitted exception to storing or using Restricted Information on a personal device. You may sync your Exchange email to your smartphone or tablet using the native email client on the device or by downloading the Outlook Exchange App to the device. See [Exchange email Setup](#). It is very important that you understand that you will then have a copy of emails on your device. In any event, the use of email for Restricted Information is strongly discouraged. You should delete any emails that include Restricted Information promptly, keeping a copy, if needed, in Box or a Tufts shared network file. See [Email Restrictions for Sensitive Personal Information](#). See Appendix B for requirements for managing your phone.

Never use Box Sync to sync Tufts information to a personally-owned device. (Note: Box Sync is becoming obsolete with the use of Box Drive.)

Only install trusted applications from reputable software providers, such as from download.cnet.com. NEVER download applications offered by email, text messages, or web links. Do not install applications offered on pop-ups from third-party websites.

E. Public Computers

Never use a public computer for Restricted Information.

F. USBs, Discs, and similar Portable Devices and Media

Do NOT use USBs, discs or similar portable devices and media for Restricted Information.

If you have used these for Restricted Information previously, see the guidelines for retiring devices.

3. Protect Information on your Devices

A. Keep it Private

1) Lock and Block

Lock devices when not in use and *block* the screen from view. Orient your computer screen away from the sight of persons passing by in your office or walking by your windows. If you are unable to do so, consider using a privacy screen that covers your device's screen from view from the side.

Log off of your computer or lock the screen whenever you are away from it, whether during the day or at the end of the day. For the simple steps to lock your computer's screen, see [Manually Locking your Computer Screen](#).

All your devices should be set so that the screen locks automatically after 15 minutes or less.

2) Don't Share your Device

Tufts-owned devices should not be shared with other persons outside of Tufts, including family members.

Never allow another person you do not know and trust to connect to your laptop or other device.

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 Support Desk, after you have contacted them.

3) Transferring Devices to a New User

Do NOT transfer a device to a new user without first having it securely wiped and then “re-imaged.” Computers and other devices store data in a complex manner that is not readily apparent to end-users. It is much safer (and easier) to have your machine wiped than to assume that you can manually find and delete all the files on your computer with confidential or sensitive data. Contact the TTS Support Desk for assistance.

4) Disposal of Computers, Printers and other Devices

Important Rule:

Before any computer, hard drive, flash drive, copier, printer, scanner, fax machine, USB, cd, other disk or other storage media is disposed of or transferred outside Tufts, it must be securely wiped or destroyed.

Computers and other devices store data in a complex manner that is not readily apparent to end-users. Often a copy of documents they have been used for can be recovered from them. It is much safer (and easier) to have your machine wiped than to assume that you can manually find and delete all the files on your computer or other device. Contact the TTS Support Desk for assistance. In some cases, Tufts contracts with the vendors for the wiping of hard drives of copiers, printers and scanners.

5) Found Devices

If you locate a computer or other device in your office that has not been used for some time and there is uncertainty about what is stored on it, do *not* turn it on or plug it into your PC or laptop. Contact the TTS Support Desk to arrange for its delivery to TTS. USBs and other devices infected with malware can be intentionally left where people may plug them into their devices.

B. Back up your devices.

Protect your Restricted Information by being sure your data is backed up to either a Tufts network shared drive or to Box. You are risking losing the documents if you only store them on your laptop or desktop, such as in “Downloads,” “Desktop,” or “Documents.” If your device is infected with malware, or your device is lost or stolen, you are likely to lose them completely. And don’t use external hard drives as your only back-up. If your desktop or laptop is corrupted by ransomware, any device connected to them, such as an external hard drive, can also be infected.

C. Update (Patch) your software. Use antivirus software.

You're responsible for making sure all your devices are well-maintained, and kept current with updates (patches) to your operating system (OS) and other software and with scans by antivirus software. Even if TTS maintains your device, you still have to apply updates (patches) for software you installed and make sure that you allow your systems to receive and install automatic updates.

Be sure to shut down and/or restart your devices each day. Many updates require a restart.

If you're using a Tufts device that isn't managed by TTS, then you are fully responsible for managing the security of that device, to Tufts' standards.

If you don't know if your device is managed by TTS, you can contact the Support Desk to find out, and to request to have TTS manage it.

4. Use Secure, Tufts Approved Apps and Tools

A. Apps, Tools and Services from Third Party Vendors and Service Providers

One way we can protect Restricted Information is to be careful about what IT apps and tools we use. For several types of Restricted Information, we're obligated by law to have the vendors agree that they will comply with specific laws. For these reasons, you should not decide on your own to start using an IT app or tool for Restricted Information. In fact, Tufts has a policy that prohibits employees from doing so.

Many of Tufts' apps and tools are authorized for use with Restricted Information. Box is approved for all Restricted Information, except for credit card data for payments to Tufts.

Qualtrics is approved for all data except i) cardholder data, and ii) data regulated under HIPAA.

DropBox, Google Drive and other Google products are not approved for use with Restricted Information.

Important Rule:

Before using a service or application that is not discussed in these Guidelines, you must confirm that Tufts has approved either that app or tool, or, for services, the vendor or other service provider, for working with Restricted Information. Contact the TTS Support Desk for more information.

This requirement applies to all third-party applications and tools, whether free or paid.

Some regulations limit what apps and tools may be used for the data protected by the regulations. The regulations require that the vendor provide written guarantees that it will use appropriate technical and organizational measures to ensure the protection of the information. These regulations include the Massachusetts Data Privacy Laws, other state privacy laws, and the General Data Privacy Regulation (GDPR) that applies to data collected from persons when they are in countries in the European Economic Area.

B. Stopping Using an Outside Service or Vendor

You should pay special attention to what arrangements are made to protect information when your office terminates any arrangement with a third-party vendor or service provider. If the vendor or provider stored or processed any Restricted Institutional Data, it is very important that Tufts receive a complete copy of that Restricted Institutional Data and that all copies the third-party has be securely destroyed. Contact the Tufts Support Desk for assistance.

C. Passwords

Always protect your passwords.

Do not use a Tufts password for any account outside of Tufts. If you have, then change your password. If the other account is compromised, your Tufts account could be compromised as well.

Remember, if you have access to Restricted Information and your password is exposed, it could be used to access valuable information about you, your colleagues and the University. Stolen passwords have been used at universities to redirect paychecks and commandeer email accounts to send spam and phishing emails to infect devices.

Do NOT share your passwords with anyone. Do NOT send your passwords in email.

Do NOT leave your passwords written on a piece of paper or a post-it.

NEVER save your passwords in any browser.

For any workstations shared within your office, always use your own individual account.

Do not use a generic password or share a common login token.

Do not use vendor supplied default passwords. Change default passwords.

Follow the Tufts Password Policy [Tufts Password Policy](#).

Use a Password Tool. There are many password tools available to help you securely store your passwords. Some are even free. Instead of leaving a written list of passwords on your desk, try one of these tools. Though it may seem insecure to keep all that information on a computer, these applications have been developed to protect your information. See [Password Tools](#).

D. Two Factor Authentication

Tufts requires you to use Two Factor Authentication to access many of its applications. Tufts 2FA is based on a solution from Duo. 2FA locks down many of the Tufts tools and apps, so that if your password is stolen, you will be protected. Logging into Tufts using Duo requires two steps: entering your userID/password and then requesting verification through Duo. More information is available at <https://it.tufts.edu/qs-twofactor>.

5. Restrict your use of email. Follow the Five: How - Who - With - What - Done

Errors in email addresses are common, which can cause Restricted Information to be sent to unauthorized persons. Email is also a frequent target of hackers. Because of the large number of emails we all receive, your inbox and outbox can be difficult to manage.

For all these reasons, your best practice is to avoid using email for Restricted Information whenever possible.

Yet, there will be times you will need to use email for Restricted Information. When you do, ask yourself:

- **How** should I send this email?
- **Who** will be able to read it?
- Should the email be sent **With** a notice or special flag?
- **What** should be included in the message or as an attachment?
- Have I deleted the email so that I am **Done**?

A. **How** to send a Restricted Information Email: Use @tufts.edu and Encryption

Important Rules:

Use your official “@tufts.edu” account if working with Restricted Information. Never use your personal email for this work.

If you have access to Restricted Institutional Data, you are not permitted to enable automatic forwarding of your Tufts email account to any other email account that is not in the university-managed email system. Do not forward a “@tufts.edu” email account to a “@abc.tufts.edu” account.

If your personal email account is compromised and Tufts’ Restricted Information is disclosed, you may be held responsible for the costs associated with the breach.

To send Restricted Information using email, the email **MUST** be sent encrypted. Three options are provided below.

1) Option 1: 99% of your Use: Stay within the @tufts.edu System

To use this option, all you need to do is send the email from an @tufts.edu address to an @tufts.edu address. If both addresses are @tufts.edu, those emails are encrypted while they are being sent.

Do not send Restricted Information in an email message if either the sending email account or the receiving email address is an address other than @tufts.edu, such as an @gmail.com address. Email accounts using @abc.tufts.edu are for a system that is separate from the University's @tufts.edu email system and should not be used for Restricted Information.

Remember never set up your Tufts email account to forward your email messages to an address outside of the @tufts.edu system.



2) Option 2: For People Outside Tufts: Using Tufts [Secure] Email

How to use Tufts [Secure] Email to Send Information to a Person Outside of Tufts

If you need to send Restricted information to someone without an @tufts.edu email address, you can use the Tufts [Secure] email tool. To use

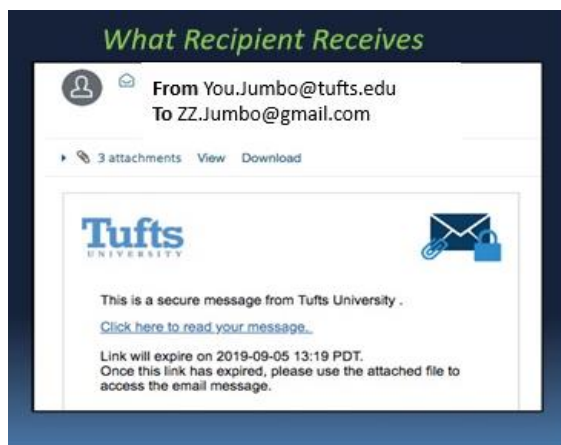
this tool, you must type the word “secure” in the subject line and add square brackets around it. The recipient will receive a link to access a secure website where they can view the information. Be sure to double check the address you are sending to because the link can be used by anyone.

It's helpful to tell the person who will receive the link to expect the message so that they don't delete it as a phish.

The [Secure] Email service will only encrypt messages sent from a @tufts.edu address to an address that is not a @tufts.edu address.

How to use Tufts [Secure] Email to Collect Information from a Person Outside of Tufts

Tufts [Secure] email also encrypts a person's reply to a message sent using the system. That means you can also use this tool to have a person outside of Tufts send encrypted information to you. For example, if you need someone to send you their passport number. First, send them an email using the [secure] email tool. Then they reply to that email to send you the information you need.



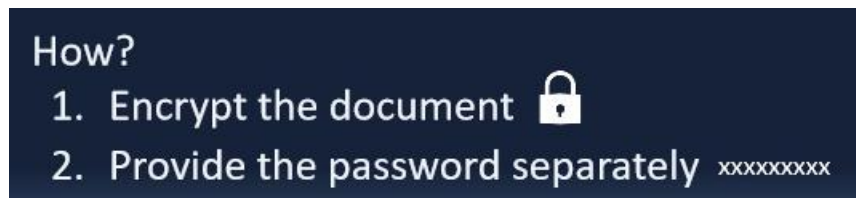
For step-by-step instructions, go to [Using Secure Email to Collect Sensitive Information](#).


3) Option 3: For Any Situation: Use an encrypted and password protected attachment

Option 3 can be used for any email you need to send, whether it is going to someone using an @tufts.edu address or someone who doesn't have an @tufts.edu address.

For example, the Restricted Information may already be in a document you can send as an attachment. Or you could type the information into a Word document, rather than in the body of the email itself.

It's a simple two-part process to send the information.



1. Encrypt the document. This is a quick process. 
 - Adobe Pro Suite gives users the ability to protect and encrypt a pdf file. See [Adobe Encryption](#).
 - Microsoft Office Suite - Word, Excel, and PowerPoint have options to protect and encrypt Office files. See [Microsoft Encryption](#).
2. Create a password that will be used to unlock the document's encryption. xxxxxxxxxxx
 - Provide that password to the recipient without using email, such as calling the person. If you regularly send an encrypted document to the same person, such as sending CORI forms to an entity outside of Tufts, you can use the same password for sending that document to the same person each time.

B. Limit **Who** will be able to Read your Email Message

- Whenever you can, only send the email to one person. Consider who really needs the information. If some information is Restricted and some related information is not, consider sending the Restricted Information in a separate email that is sent only to the person who needs it, while the related information is provided to the others who are also working on the project.
- The best practice is to avoid using elists for sending Restricted Information. Elists can quickly become out of date and include people who should not receive the information.
- Check the email address you are sending to, and then check again. If an email has Restricted Information and it is sent to someone who should not have received the information, that may be reportable as a data breach. If this happens, take the actions in Section III.10 about reporting a possible data breach.

- It's good practice to always start with a new email, rather than continuing a thread. Be very careful with "Reply" and "Forward." When Restricted information is included in a chain of emails, the information can become "buried" and may be inadvertently sent to someone who should not receive it.

C. Consider sending the Email **With** a Special Notice or Flag

To alert the email's recipient to the sensitivity of the information, it is good practice to include a message such as:

"This message contains material that is confidential for the sole use of the intended recipient. Any review, reliance or distribution by others or forwarding without express permission is strictly prohibited. If you are not the intended recipient, please contact the sender and delete and destroy all copies."

You may also want to send the email flagged as High Priority so it is not overlooked and is read promptly.

D. Limit **What** is included in the Email

Before sending the email, review what you have included and delete any Restricted Information the recipient doesn't need for their Tufts' work. For personal information, when possible, don't include the person's name. If some identifier is necessary, consider using only initials or a partial name.

E. Securely Delete the Email to be **Done**

Don't store Restricted Information in email. Don't use email as a file system for important information.

Use these 3 steps to completely delete an email so that it is not recoverable:

1. Place the email in Trash
2. Empty the Trash
3. Purge your Trash so the email can't be recovered. See [Securely Deleting Email](#).

F. Using Tufts Email on your Personal Smartphone, Tablet and other Devices

You may sync your Tufts Exchange email to your smartphone or tablet using the native email software client on the device (i.e. the software already loaded on your device) or by downloading the Outlook Exchange App to the device. It is very important that you understand that you will then have a copy of emails on your device. See [Email Restrictions for Sensitive Personal Information](#). If you are not using a Tufts-managed laptop or desktop and you need to access your Tufts email, then you should *only* use the Outlook Web App, by going to: <https://exchange.tufts.edu>. This will provide you an encrypted connection to your email. It is also protected by Two-Factor Authentication (Duo).

G. Accessing your Tufts Email Off Campus on your Tufts Device

If you are using a Tufts-managed device, you may use either the Outlook software client on your device or the Tufts email website. It is highly recommended that you also use the Tufts VPN.

6. Use Tufts_Secure WiFi and the Tufts VPN

A. WiFi

When using wireless on campus, **ONLY use Tufts_Secure**, which is encrypted.

Do NOT use Tufts Wireless or Tufts Guest; they are not encrypted.

B. Virtual Private Network Connection for Working Off-Campus

When working off-campus, use the Tufts VPN to connect to Tufts services. In some limited situations, a Data Authority may expressly authorize the use of an “https” secured site or similarly encrypted service for specific types of information.

7. Print and Scan with Care

A. All Copiers, Printers, Scanners and Fax Machines

1) Protect the Documents

In most cases, copiers, printers, scanners and fax machines keep a copy of the information that is copied, printed, scanned or faxed by them in their memory. For this reason, only use Tufts supplied or approved copiers, printers, scanners and fax machines, or machines that you control.

Immediately pick up any documents sent to a printer. Do not leave any documents unattended.

Any copier, printer, scanner or fax machine used for Restricted Information must be located in a work area during the workday and in a locked space after the workday ends.

Limit the number of copies made to as few in number as possible.

2) Consider using a Password on the Machine

Most Tufts supplied printers may be configured for password protected printing. Secure Print on Konica machines will delay printing a document until you enter a password at the printer. Contact the TTS Support Desk for help setting up a printer for Secure Print.

3) Have Machine Wiped Before Disposing or Donating

Always have the machine’s hard drive wiped before disposing of or donating the machine. Our printer supplier of leased machine has agreed with Tufts to securely wipe all of its machines when they are returned.

B. Special Rules for Sending Restricted Information Using Fax

Use a fax cover sheet that includes a confidentiality statement. Do not include any Restricted Information in the cover sheet. For example:

“This fax contains material that is confidential for the sole use of the intended recipient. Any review, reliance or distribution by others or forwarding without express permission is strictly prohibited. If you are not the intended recipient, please contact the sender and delete and destroy all copies.”

Always confirm the:

- The recipient’s number
- That there are secure arrangements for receiving the fax, e.g. the machine is kept in a private area.
- That the fax has been received receipt of the fax.

8. Protect your Paper Documents

A. Keep Offices Physically Secure

Your department is responsible for using strong controls to protect paper records that include Restricted Institutional Data.

Only give access to office spaces to authorized persons.

Access to keys, as well as codes for alarms, doors, and lockboxes, must be limited to only those persons who must use them to do their work. When a person who had access to codes has left your office, it is strongly recommended that the code or other security method be changed immediately. Report lost or stolen keys or identification cards to Tufts Public and Environmental Safety immediately.

B. Protect Paper Documents when Working with Them

Protect all documents with Restricted Information from view by passersby and others. Do not leave them unattended in an unsecure area.

When you step away, block them from view or lock them up.

C. Use Two Locks for Paper Documents.

Always lock paper documents with Restricted Information in a secure place at the end of the workday. Paper records with Restricted Information must be secured by being stored in a locked file cabinet, drawer or other container, that is located in a locked space (the two-lock standard).

D. Shred Securely

Shred using one of the following:

- a micro-cut (this is preferred) or cross-cut shredder that cuts in two directions, into squares or rectangles. Don’t use a shredder that cuts in strips like linguine.

- Secure disposal bins from Shred-it, the only Tufts approved vendor. Keep the bins in a secure location.

9. Be prepared for rights requests

Some privacy laws give individuals the right to access the information Tufts has about them.

A. Student Requests under FERPA

Students have rights under FERPA to view their educational records. If a student makes a request to do so, direct them to their school's Registrar office. Students may also request a "privacy block," which limits access to their information by others. Information is available from each school's Registrar office about how to establish a privacy block.

Always remember that if you are sharing information about students, even within Tufts, to consider whether any of the students have filed a privacy block.

B. Requests under the European Union's (EU) General Data Protection Regulation (GDPR)

The EU's GDPR grants individuals the right to view the personal data the University has about them, if that information is within the scope of the GDPR. For example, if personal information is collected from someone when they are in one of the countries of the European Economic Area, that information is protected by the GDPR.

Individuals may also have a right to have the information Tufts has about them erased or to have Tufts stop using the information. If an individual requests to exercise a right under the GDPR, the University has a limited period of time to respond. When a request is received, the University will review what information is protected by the GDPR, what exceptions apply, and what offices and departments need to be included in responding to the request.

Since each request may take a considerable amount of time and work to evaluate and respond to, it's important to send the information about the request to dataprivacy@tufts.edu within 24 hours. This includes requests you might receive in writing or that are made verbally.

More information about the GDPR is provided in Section V. **ADDITIONAL REQUIREMENTS FOR EEA PERSONAL DATA PROTECTED BY THE GENERAL DATA PROTECTION REGULATION (GDPR).**

10. Immediately report any potential security incidents

Immediately report any potential security Incident involving Restricted Information to the TTS Support Desk by phone at 617 627-3376.

If there is a personal data breach, privacy regulations generally require the disclosure be reported within a short period of time. For example, the EU's GDPR requires that Tufts report the breach "without undue delay and, where feasible, not

later than 72 hours after having become aware of it, ... unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.”

In order to meet these requirements and to protect the individuals that may be affected, it is extremely important that you report any security incident that involves Restricted Information immediately to the TTS Support Desk. Use the phone number rather than the email address. TTS Information Security will then work with University Counsel to evaluate the report.

For more information, see [Reporting an Information Security Incident](#).

Examples of security incidents include:

- Loss or theft of a laptop, desktop or other equipment used to access or store Restricted Information, including a mobile phone, thumb drive, external hard drive or printer
- Intrusion into a computer system
- Unauthorized access to Restricted Information, whether intentional or accidental
- Unauthorized use of another user’s credentials or impersonating another university user
- A compromised user account
- If you are unsure whether an event is a security incident, it is best to err on the side of caution, and report the event to the TTS Support Desk.

You may also report suspected unauthorized disclosure or use of Restricted Institutional Data anonymously, through [EthicsPoint](#).

IV. SPECIAL RULES FOR SENSITIVE PERSONAL INFORMATION (SPI)

1. Social Security Numbers

A. Special Uses

Social Security numbers (SSNs) are especially sensitive data and should be rarely used. TTS has been implementing new tools to limit the usage of SSNs across the university. For most work at the University, you will never need to collect or view an SSN.

B. Last Four Digits

Restricted Information includes SSNs with all nine digits. In some limited cases, it may be necessary to collect the last four digits of an SSN, and that information is not specifically regulated at this time. Yet, that practice is discouraged and should be avoided whenever possible. In some cases, the last four digits of an SSN are sufficient to be able to determine the full nine digits of an individual’s SSN, based on known algorithms for determining SSNs.

C. Use of Social Security Numbers as Student ID Numbers

For many years, Social Security numbers (SSNs) were used as student ID numbers at Tufts, as they were at other universities. Older student records at Tufts may unexpectedly contain SSNs. For that reason, be especially careful maintaining the privacy of those records. In some cases, it may also be prudent to redact the SSNs. See Section III.1.D.7: Removing or Redacting Information in Electronic Documents without Deleting Document, and Section III.1.D.9: Removing or Redacting Information from Paper Documents.

2. Local Office and Departmental Policies

Each office and department is strongly encouraged to have a local policy that specifically restricts access to SPI to specific persons. Many offices and departments have these policies, and a copy of the policy is available from the Information Steward.

3. Only Use Apps and Tools approved for use with SPI

Before using an IT app or tool for SPI, you will need to think about whether the configuration of the app or tool will enable the third-party vendor to access or store the information. Will the vendor store the information on its servers, i.e. in the cloud? If the vendor will store or otherwise process SPI, there must be documentation of the vendor's compliance with the Massachusetts Data Privacy Laws. That documentation must include a written agreement to abide by those laws. The SPI must be encrypted when stored on portable devices and when transmitted wirelessly or across public networks.

4. Incident Reporting

A. Reporting Period; Affected Persons

The Massachusetts Data Privacy Laws require the reporting of a security breach involving personal information as soon as practicable and without unreasonable delay. Similar laws in other states use the same standard or a specific time period, such as 30 or 60 days. In Massachusetts, a report is required even if only one person is affected.

For these reasons, it is especially important that a possible security incident be reported immediately by phone to the TTS Support Desk at 617 627-3376. See Section III.10: Immediately report any potential security incidents.

B. Reporting of Persons Involved

The Massachusetts Data Privacy Laws now include a provision that requires the reporting of the person responsible for the breach of security, if known.

V. ADDITIONAL REQUIREMENTS FOR EEA PERSONAL DATA PROTECTED BY THE GENERAL DATA PROTECTION REGULATION (GDPR)

This section explains some of the key concepts and terms used by the GDPR. You can also learn about the GDPR on Access Tufts at [GDPR Information](#) and by reviewing the [GDPR FAQs](#).

If you have questions about the GDPR, please send your inquiry to dataprivacy@tufts.edu. This section includes six of the GDPR's requirements. Many of these are similar to the 10 strategies discussed in Section III: Key Strategies for Restricted Information.

1. Know when your work requires complying with the GDPR

A. GDPR and Collecting Personal Data when a Person is in the EEA

When an individual is in the EEA, any Personal Data collected from them in connection with the offering of a good or service – such as providing an education - is protected by the GDPR. All persons are protected; there is no requirement that the person be a resident of the EEA or a citizen of a country in the EEA. Protection for the Personal Data continues after the person leaves the EEA.

B. GDPR and Established Programs in the EEA

If Personal Data is collected or otherwise processed in the context of the activities of any establishment in the EEA, then the Personal Data is protected by the GDPR, even if the processing occurs outside the EEA. Examples of establishments in the EEA include Tufts-sponsored study abroad programs in Europe.

C. GDPR and Collecting Personal Data When Monitoring a Person's Behavior

The GDPR protects a person's Personal Data when the Personal Data is collected by monitoring the individual's behavior while they are in the EEA. Monitoring would include tracking behavior across a website.

D. The GDPR and Conferences

Presenters and attendees at a conference from the EEA will provide the conference organizers with Personal Data protected by the GDPR. For information about complying with the GDPR for conferences to be held in the US, see [GDPR \(General Data Protection Regulation\) Considerations for Tufts Conferences Occurring in the US with Promotion in or Attendees from the European Economic Area \(EEA\)](#).

E. The GDPR and Research

Information for researchers may be found at [GDPR for Researchers](#), including [GDPR FAQs for Researchers](#).

F. The GDPR and Mailing Lists

Email addresses and other information collected for a mailing list is Personal Data under the GDPR. If your office manages a mailing list, review [GDPR\(+\)
Tasks for Tufts University Mailing Lists](#) for information on complying with the GDPR.

G. What is EEA Personal Data?

The GDPR applies to all EEA Personal Data, which includes any information relating to an identified or identifiable person. Examples include:

- Name
- Social Security numbers and other identification numbers
- Email addresses
- IP addresses
- Location data
- Information collected by online cookies
- Images

Generally, personal data is protected even if it has been otherwise publicly disclosed.

H. What is “processing” under the GDPR?

“Processing” under the GDPR includes any ways of working with the information, including collecting, storing, and sharing the information.

2. Minimize collecting, using and sharing EEA Personal Data

A. Limit EEA Personal Data

Strategy 1 for Restricted Information, that is, Focus on what Information is Needed, is a core principle of the GDPR. This is often called “data minimization.” The GDPR requires that we eliminate or reduce the amount of EEA Personal Data we collect, use, and store as much as possible. EEA Personal Data may only be “processed,” that is, worked with in any way, if there is a justification for having the information. Also, you may only share EEA Personal Data with persons who *need to know the information for their job responsibilities*. You shouldn’t disclose or give access to EEA Personal Data to someone who does not need it.

B. Anonymize and Pseudonymize

Anonymized information is not “personal data” under the GDPR. Unfortunately, the GDPR doesn’t describe the practices that it considers adequate to anonymize information. Instead it relies on a general standard: under the Regulation, anonymous information neither identifies an individual nor makes it possible to identify an individual.

HIPAA de-identified information will be considered pseudonymized personal data under the GDPR, not anonymized.

So long as a key exists to re-identify information, even if the key is sequestered from the research team, the information will not qualify as anonymized.

If anonymization is not feasible, the GDPR encourages pseudonymization of personal information to protect the individuals. Under the GDPR, data is pseudonymized if:

- The information cannot be attributed to a specific individual without the use of additional information (i.e. a “key”)
- The key is kept separately from the data set
- Access to and use of the key is protected by technical and administrative measures. The key must be kept separately, but designated, authorized persons within the research team may have access.

C. Develop and Follow a Data Retention Plan

The GDPR requires a data retention plan for all personal data. Personal data should not be kept “longer than is necessary for the purposes for which the personal data are processed.” (Ch. II. Art. 5.1.(e))

See Section III.1.D Keep only What you Need – When and How to Store Restricted Information of these Guidelines for more information about records retention.

3. Have a permitted Justification under the GDPR for processing Information

You must always have a documented, *lawful basis – i.e. a justification* - for working with EEA Personal Data.

You must also have a justification whenever you share EEA Personal Data.

The GDPR provides several alternatives for a lawful basis for EEA Personal Data that is not Special Category Information. These three justifications are the most common for working with the most common types of EEA Personal Data:

- It is necessary for a legitimate interest of the University
- It is required in connection with a contract
- The individual has consented to the processing (appropriate only in limited situations)

A. Working with Personal Data is Necessary for a Legitimate Interest of the University

This is the broadest justification under the GDPR for collecting and processing personal information. We rely on this justification for many of Tufts’ activities and programs.

B. Working with EEA Personal Data is Necessary in Connection with a Contract

This justification applies when working with EEA Personal Data is required to meet Tufts' obligations under a contract with the individual. For example, a legal basis for collecting personal data from students in our Study Abroad programs is that Tufts and the student have agreed to the student participating in the program.

C. The Individual has Fully Consented to Tufts' Processing their Information

In the US, it is common practice to rely on consents given by an individual as a justification for using their personal information. In the EEA, consent is treated differently. Often consent will not be held up as effective and binding because it is viewed as not being freely given on a fully informed basis. Generally, there cannot be any penalty for withholding consent, such as a denial of access to a service.

Even when consent may be used, often the person is free to withdraw it at a later time. If consent is withdrawn, any future use of the information will be prohibited.

Therefore, whenever possible, Tufts' approach is to rely on either the legitimate interest or the contract legal basis for our GDPR activities.

4. Give a Disclosure Notice

When Tufts processes EEA Personal Data, the data subjects are entitled to an informational notice disclosing what personal information will be collected; the purposes for which it will be used; the lawful basis, i.e. justification; with whom it will be shared; and how long it will be retained, as well as information about an individual's rights under the GDPR and how to exercise them.

To meet this requirement for many of our most frequent uses of EEA Personal Data, Tufts has prepared several EEA Privacy Statements. These are posted at <https://www.tufts.edu/about/privacy> and Tufts' websites generally include a Privacy link for users to easily locate these Statements.

In many cases it will be useful to add text to a website page, a form or application, or other material to draw the attention of the person whose data is being collected to the Statements and/or to include additional information. In other cases, such as for research studies, a longer notice will often be appropriate.

5. Follow Stricter Requirements before Collecting or Using Special Category Information

Before you collect or use EEA Personal Data that is in one of the following sensitive categories, you must confirm the collection and use of the information will comply with the GDPR. The GDPR imposes stricter requirements on these types of information. Consult with the persons responsible for GDPR compliance in your

program or area. Questions may also be sent to the University's Data Privacy Team at dataprivacy@tufts.edu.

Whenever possible, it's recommended to not collect or use these types of sensitive information when the GDPR applies.

The following information is treated as sensitive or Special Category Information under the GDPR:

- Racial or ethnic origin
- Physical or mental health data
- Political opinions
- Sex life and sexual orientation
- Religious or philosophical beliefs
- Trade union membership
- Genetic and biometric data (e.g. fingerprints, or facial recognition data)

Important Rule:

In most cases, the GDPR will prohibit the collection and use of criminal conviction and offense information from or about persons while they are in the EEA or in connection with one of our established programs in the EEA.

6. Only Use Apps and Tools approved for use with EEA Personal Data

Before using an IT app or tool, you will need to think about whether the configuration of the app or tool will enable the third-party vendor to process the information. For example, will the vendor store the information on its servers, i.e. in the cloud? If the vendor will store or otherwise process EEA Personal Data, there must be documentation of the vendor's GDPR compliance.

The GDPR's requirements may also limit how you use an otherwise approved app or tool. Apps and tools that store data outside of the EEA, but are used by research subjects to submit information while they are in the EEA, will generally be considered as causing a transfer out of the EEA. Examples include Qualtrics and Box. It's recommended that a consent to the "transfer" of that data out of the EEA be obtained either before the app or tool is used, or in the case of a survey tool, as the first action of the person using the tool. Contact dataprivacy@tufts.edu for assistance.

7. Have Written Agreements with Third Parties with whom you Share Personal Data

If your office shares any EEA Personal Data with a non-Tufts organization, then you will need to have them agree in writing that they will comply with the GDPR

when storing or working with information. Examples include storing paper copies off-campus or collaborating with another university.

8. Follow the requirements for transferring EEA Personal Data from the EEA to the US.

Before you transfer EEA Personal Data from the EEA to the US, you must confirm the transfer will comply with the GDPR. Consult with the persons responsible for GDPR compliance in your program or area. Questions may also be sent to the University's Data Privacy Team at dataprivacy@tufts.edu.

Whenever possible, collect personal information when the person is in the US so that a transfer to the US is not required.

To properly transfer EEA Personal Data:

- There must be a valid justification that applies for Special Category Information. The most common of these are:
 - The person whose data it is has explicitly consented to the proposed transfer, after having been informed of the possible risks of the transfer. The consent may usually be withdrawn at any time.
 - The transfer is necessary for the performance of a contract with the person whose data it is.
 - The transfer is necessary for the establishment, exercise or defense of legal claims.
- Only use applications and information services that are approved for use with EEA Personal Data.
- The GDPR notice to the data subjects should disclose that personal data will be transferred out of the EEA.
- If the personal data includes Special Category Information (described above), then consult with the persons responsible for GDPR compliance in your program or area. Questions may also be sent to the University's Data Privacy Team at dataprivacy@tufts.edu.

9. Know the GDPR Rights for Individuals. Immediately Report Rights Requests.

Strategy 9 – Be prepared for Rights Requests – is especially important for the GDPR. The GDPR provides the following special rights for individuals with respect to their EEA Personal Data. These rights are limited to EEA Personal Data; they do not apply to other personal data Tufts may have about them.

A. The GDPR Rights Individuals may Exercise

The GDPR rights are:

- The right of access. The right to a copy of all of the EEA Personal Data that Tufts has about a person. This right is subject to some limitations, including that providing a copy will not adversely affect the rights of others.

- The right to correct. The right to have inaccurate EEA Personal Data corrected, or completed, if it is incomplete.
- The right to erasure (also known as the right to be forgotten). The right for a person to have their EEA Personal Data erased. This right is not absolute and has important exceptions for when it does not apply.
- The right to restrict processing. The right to request that access by others to a person's EEA Personal Data be restricted. This is not an absolute right and only applies in certain circumstances. If processing is restricted, Tufts would generally not be permitted to use the information without the individual's consent. Exceptions include needing to use the information in connection with a legal claim or to protect another person.
- The right to data portability. This right would permit a data subject to be given an electronic copy of their EEA Personal Data so that they are able to reuse that data for their own purposes outside of Tufts. The GDPR provides this right so that a person may easily move, copy or transfer EEA Personal Data easily from one IT environment to another. This right only applies to information an individual has provided to Tufts and depending on the context, applies to some of their information, but not to all of their information.

B. Submitting a Rights Request

Individuals may exercise their rights verbally or in writing. If you or your staff receives a request, then:

1. Let the person know that they can find information at <https://www.tufts.edu/about/privacy>, including a form to assist them with making a request; and
2. Also, send an email describing the request that was already made to dataprivacy@tufts.edu, immediately, and in any event, within 24 hours.

10. Immediately report any potential Security Incident involving EEA Personal Data or other Restricted Institutional Data to the TTS Service Desk

When combined with a person's name, EEA Personal Data may be used for identity theft or fraud. If there is a personal data breach, the GDPR requires that Tufts report the breach "without undue delay and, where feasible, not later than 72 hours after having become aware of it," to the EEA authority, "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."

In order to meet these requirements and to protect the Data Subjects that may be affected, it is extremely important that you report any security incident that involves EEA Personal Data immediately to the TTS Service Desk. Use the phone number rather than the email address. TTS Information Security will then work with University Counsel to evaluate the report.

For more information, see [Reporting an Information Security Incident](#).

For examples of security incidents, see Section III.10.

You may also report suspected unauthorized disclosure or use of Restricted Institutional Data anonymously, through [EthicsPoint](#).

VI. SPECIAL SITUATIONS

1. What to do if you receive Restricted Information that you did not request

Contact the sender and determine why the information was sent to you. Request that the sender stop sending the information.

Either securely store the information or dispose of the information. See the guidelines for securely storing and disposing of documents.

2. Working off campus and telecommuting

When you work remotely, that is, off campus, you are responsible for protecting Tufts data and systems. This includes if you are working with information that is stored off-campus, such as on your laptop, or if you are working with information or systems that are located on campus in Tufts facilities that you are accessing remotely. Follow the [Guidelines and Services for Working Off Campus or Telecommuting](#). Also see the requirements described above for using a personal PC or laptop for Restricted Information in Section III.2.D.

3. Employees leaving your Office

Before an employee leaves, it is good practice to request that the employee review their email to determine if there is important information included in their mailbox that is not stored in another location, such as a folder in Box or a shared network drive, that their colleagues will need to continue the employee's work. In most cases, a former employee's email records will be deleted after 30 days.

Every separated employee must:

- Return all records containing Restricted Information in the employee's possession (including all information stored on laptops or other portable devices or media, and in files, records, work papers, etc.).
- Surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to Tufts premises or information, except to the extent expressly approved in extraordinary circumstances for a particular individual by a senior administrator.
- Return any laptop, desktop or other device that was purchased by Tufts, unless expressly approved in extraordinary circumstances for a particular individual by a senior administrator. When the device is returned to Tufts, it should always be sent to TTS to have the hard drive securely wiped before being re-

provisioned, retired, donated, disposed of or recycled. Do not just transfer the laptop or other device to another employee. If the employee is granted permission to retain the device, the hard drive must first be securely wiped by TTS to remove Tufts institutional data.

- Disable all physical and electronic access by the individual to Restricted Information as soon as possible, including remote access.
- When a person who had access to codes, such as for an alarm, door or lockbox has left your office, it is strongly recommended that the code or other security method be changed immediately.

VII. HOW DO YOU GET HELP?

1. Information Stewards

Most Tufts offices have a designated Information Steward trained in working with Restricted Information. When you have questions about the best practices to use, you can contact your Information Steward for assistance. You can find a list of the University's Information Stewards at: [Information Stewards Contact List](#).

2. TTS Website

The *TTS website* at it.tufts.edu includes instructions and guidance on using Tufts' information systems and applications.

3. TTS Support Desk

Questions about the Tufts information systems and applications can also be submitted to the *TTS Support Desk* 617 627-3376 or email or it@tufts.edu.

4. GDPR Consultations

For advice on working with Restricted Information, you can consult with the persons responsible for GDPR compliance in your program or area. Questions may also be sent to the University's Data Privacy Team at dataprivacy@tufts.edu.

Appendix A: European Economic Area (EEA) Countries

(as of September 9, 2019)

Austria	Latvia
Belgium	Lichtenstein
Bulgaria	Lithuania
Croatia	Luxembourg
Cyprus	Malta
Czech Republic	Netherlands
Denmark	Norway
Estonia	Poland
Finland	Portugal
France	Romania
Germany	Slovakia
Greece	Slovenia
Hungary	Spain
Iceland	Sweden
Ireland	United Kingdom
Italy	

In most situations, Switzerland's privacy laws require protections similar to those of the GDPR.

Appendix B: Required Strong Controls for Personal Devices or Tufts Devices

<p>Require a Password for access to your device and Use a Strong Password</p>	<p>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 Password Tools.</p>
<p>Manually Lock your Screen or Power Off when you leave your device</p>	<p>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 Manually Locking your Computer Screen.</p>
<p>Set your Screensaver to Automatically Activate</p>	<p>You should configure an automatic screen lock on your devices that requires you to enter a password to resume using the device after 15 minutes or less.</p>
<p>Review Privacy Settings</p>	<p>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.</p>
<p>Apply Updates/Patches</p>	<p>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).</p> <p>Configure automatic updates wherever possible, and when patches are finished installing, follow any prompts to reboot the device to ensure proper functionality.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Windows updates and other protection tools and advice can be obtained at: http://www.catalog.update.microsoft.com/Home.aspx <input type="checkbox"/> Apple updates are available at: http://support.apple.com/kb/HT1222 or via iTunes <p>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.”</p>

<p>Install and use Antivirus Software</p>	<p>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</p> <p>There are many other vendors with inexpensive options such as McAfee or Norton and free options such as AVG, Malwarebytes, Avast, Sophos and Bitdefender. When downloading free software, use a trusted website, such as download.cnet.com.</p>
<p>Install a Firewall</p>	<p>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.</p>
<p>Only Install Trusted Applications</p>	<p>Only install trusted applications from reputable software providers, such as download.cnet.com.</p>
<p>Use Secure WiFi and Bluetooth Settings</p>	<p>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.</p> <p>Be aware that Wi-Fi Sense, which is part of older version of Windows 10, may share access to your networks with others and connect you to open networks automatically. Do not use the Express settings. Customize your settings and uncheck the options you don't want. See https://www.lifewire.com/what-is-wifi-sense-windows-10-4586925.</p>
<p>Limit Sharing of Devices</p>	<p>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 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.</p>

<p>Physically Protect all Portable Devices</p>	<p>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.</p>
<p>Do Not Allow other Persons you do not Know and Trust to Connect to your Devices</p>	<p>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 Support Desk, after you have contacted them.</p>
<p>Securely Erase all Personal Devices when Your Use Ceases</p>	<p>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.</p>
<p>Return any Tufts owned Device when Your Employment Ends</p>	<p>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.</p>