QUICK GUIDE
RESTRICTED INFORMATION HANDLING

Making confidentiality and privacy part of your daily work

Strategy 1:
Focus on What is Needed

- *Collect* only what is needed
  - More is not better
- *View* only what is needed
  - Don't look up information out of curiosity
- *Keep* only what is needed
  - Follow the retention schedules
- *Share* only what is needed
  - Limit access to files

Strategy 2:
Only Use Secure Devices

- Encrypt your Tufts laptop. Contact the TTS Support Desk.
- Don't use any Tufts device for Restricted Information unless it is managed by TTS or follows TTS standards
- Don't store Restricted Information on your personal devices – except in Tufts email on a secure smart phone

Strategy 3:
Protect Information on Your Devices

- *Keep it private: Lock* your screen and *Block* your screen from sight
- *Back up your data: Use* Tufts Network Drives or Box or other University approved locations
- *Update* your operating system and applications by applying software patches
- *Wipe all devices* before changing the assigned user or disposing of the device

Strategy 4:
Only Use Tufts Approved Apps and Tools

- Only use IT apps and tools approved for Restricted Information
- Box is approved **except** credit card data and some research data
- Qualtrics is approved **except** for HIPAA, cardholder, and some research data
- Don't use DropBox or Google tools for Restricted Information
- Protect your password. Don't share it with anyone. Don't have a group password. Use a unique password for your Tufts work.
- If your office stops using a vendor, be sure any shared Tufts information is retrieved and the vendor destroys any copies.

Strategy 5:
Restrict Your Use of Email

- Avoid using Email whenever possible
- Don't store Restricted Information in email – delete or move the messages
- Don't use your personal email for Tufts Restricted Information
- If you use email for Restricted Information, send it encrypted – chose 1 of 3:
  1. Stay within the @tufts.edu system
  2. Use an encrypted, password protected attachment
  3. Send from @tufts.edu to outside @tufts.edu system using [Secure] in the subject line

See Restricted Information Handling Guidelines.

Strategy 6:
Use Tufts_Secure WiFi on Campus And Tufts VPN Off Campus

- When using WiFi on campus, only use Tufts_Secure. It's the only encrypted Tufts WiFi.
- Off campus? Need to connect to a Tufts service? Always use the Tufts VPN.

Strategy 7:
Print and Scan with Care

- Only use Tufts approved copiers, printers and fax machines
- Dispose of printers, scanners and fax machines securely – if there's a hard drive, be sure it's wiped
- Pick up copies immediately
- Copiers should be in a secure place

Strategy 8:
Protect your Paper Documents

- Store the information securely. Use two locks for paper documents with Restricted Information
  - Locked file cabinet or desk
  - Locked office or other space
- Use cross-cut shredders or Shred-It bins
- Keep offices physically secure
- Keep papers out of view of passersby

Strategy 9:
Be Prepared for Rights Requests

- Students have rights under FERPA to view their information. Contact the school registrar.
- Individuals have personal data rights under European Data Privacy Law (GDPR) – Report any verbal or other requests to dataprivacy@tufts.edu within 24 hours

Strategy 10:
Report Possible Data Breaches and Information Security Incidents

- Report any potential data breach or other information security incident involving Restricted Information **immediately** to the TTS Support Desk: 617 627-3376
- See the Reporting Information Security Incidents Guide on it.tufts.edu

Where to Get Help and Find More Information

- Restricted Information Handling Guidelines
- *AccessTufts* at access.tufts.edu/
- *TTS website* at it.tufts.edu
- Your Information Steward. See the Information Steward Contact List.
- TTS Support Desk:
  617 627-3376 or it@tufts.edu
- GDPR Consultations:
  Email dataprivacy@tufts.edu