THE
NEW
SCHOOL

Information Security Tips for Working Remotely

Which computer(s) should I use?

During the COVID-19 coronavirus outbreak, The New School has temporarily relaxed its requirements to use only university-issued laptop and virtual desktop computers to access New School systems and services and work with New School information.

Employees who have not been provided with a university-issued laptop or virtual desktop computer may use their personally owned computer or mobile device to work remotely until the all-clear has been given to return to normal office work routines. However:

1. Laptop and desktop computers must be running a currently supported operating system. This means Windows 8, Windows 10, Mac OS X 10.13 (High Sierra), 10.14 (Mojave), or 10.15 (Catalina) ***only.*** Windows XP, Windows 7, and Mac OS X 10.12 (Sierra) and below are ***not acceptable.***
2. Laptop and desktop computers must be up to date on security patches. On Windows, run Windows Update to install patches. On Mac, run System Preferences→Software Update.

Any employee owned computer or mobile device used to access New School systems or services must be protected with a locking screen saver, security code or pattern, or biometric authentication (fingerprint, facial recognition).

What training should I take?

We recommend that you take the New School information security awareness training, *What You Need to Know About Information Security,* before you begin working remotely. If you are going to be using the New School VPN, completion of this training is mandatory. You can access the training at https://infosectraining.newschool.edu/.

If you will be working with student education records, we also recommend that you refresh your knowledge of the Family Educational Rights and Privacy Act by completing the New School FERPA training, which you can access at https://www.newschool.edu/ferpa/quiz/.

What policies should I know about?

When working remotely (and also when working on campus), every employee is responsible for abiding by:

- The New School Information Security Policy
- The New School Information Resource Acceptable Use Policy
- The New School General Controls for Handling Sensitive Information

These documents can be found on the IT website at https://it.newschool.edu/services/security/information-security-policies-and-standards/.

Where should I work on confidential information?

The best places to work on New School confidential information are the ones that don't require you to store that information on your computer's local hard drive. In order of preference, you should store and work on files containing New School confidential information:

1. On your department's network file share ("S Drive"). Note that you must be connected to the New School VPN to access network file shares.

   Since you're not using a university-issued computer, you will have to manually "mount" network file shares to access them (this is done automatically on university-issued computers). To do this, follow the instructions at:

- Windows computers: https://it.newschool.edu/services/office-technology/network-share-drives/how-to-connect-your-windows-pc-to-network-drive/
- Mac computers: https://it.newschool.edu/services/desktop-support-and-office/network-share-drives/how-to-connect-your-mac-to-network-drive/

Alternatively, you may want to open a remote desktop session to your office computer, which already has the network shares mounted. You can also do this if you need access to software that's not installed on your personally owned computer. To open a remote desktop session to your office computer, follow the instructions at https://it.newschool.edu/services/security/virtual-private-network-vpn/waking-computer-remote-vpn-access/.

2. On the New School G Suite platform (Google Drive, Google Docs, etc.). Note, however, that some very sensitive information, such as Social Security numbers, bank account numbers, and health information, should not be stored in G Suite.

3. If neither of the above options is workable, on your local hard drive.

   If storing or working on New School confidential information on your local hard drive is absolutely necessary, you should create a single, top-level folder where you will put all these files (you can make subfolders too, if you want). That way all the university information will be in one, easy-to-find place so that when you return to the office, it will be easy to copy the information to a New School computer or file server and delete it from your personally owned computer.

What should I ***not*** do?

- Do not upload, create, store, or send New School confidential information to unofficial, non-university cloud services. The license agreements for these services do not provide legal protection or accountability for New School information. They also generally do not comply with the information security and privacy safeguards required by state, federal, and international laws and regulations or university policies. Some of the more common services in this category include, but are not limited to, Dropbox.com, Box.com, Apple iCloud, Microsoft OneDrive, Office 365, Adobe Creative Cloud, and the consumer Google G Suite platform.
- External email service providers, including Google's consumer Gmail platform (`@gmail.com`), do not provide legal protection or accountability for New School information, and they generally do not comply with the information security and privacy safeguards required by state, federal, and international laws and regulations or university policies. ***New School employees (including faculty) may not automatically forward or redirect messages from an official university email address (containing `@newschool.edu`) to a non-university email address (containing anything other than `@newschool.edu`).*** Doing so may put that individual and The New School at risk of violating state, federal, or international laws and regulations.

IF YOU HAVE QUESTIONS OR PROBLEMS, CONTACT IT CENTRAL AT
itcentral@newschool.edu OR 646.909.4357