# Information Security Tips for Working Remotely

## Which computer(s) should I use?

The New School requires that employees working remotely use a university-issued laptop or virtual desktop to access New School systems and services and work with New School information. University-issued computers have specific security measures installed to help protect university information, including the personal data of students and employees, from unauthorized access.

Employees' personally owned computers and mobile devices ***may not*** be used to work remotely, with the following exceptions:

1. Employees may use their personally owned computers and mobile devices to access New School email (Google) to send and receive messages, either via a web browser (desktops and laptops) or the official Gmail app (mobile phones and tablets). In either case, file attachments should only be viewed inside the browser or app; they should not be downloaded to the local system.
2. Employees may use their personally owned computers and mobile devices to access the New School telephone system using the Jabber softphone client to make and receive telephone calls.

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. But, university-issued laptops have been configured to protect files downloaded to local storage, so it's okay to do that when necessary. 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.

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. On your local hard drive.

## 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**