Where Should I Store This File?

	Work-Related Files & New School Information			Personal Files	
	Unrestricted	**Restricted**	**Confidential**	**Documents**	**Music & Photos**
Local PC hard drive	**OK** for work in progress	**OK** for work in progress	**OK** for work in progress	**OK**	**OK**
Personal network drive	**OK**	**OK**	**OK**	**OK**	**NO**
Department network share	**PREFERRED** for "master" copies and shared files	**PREFERRED** for "master" copies and shared files	**PREFERRED** for "master" copies and shared files	**NO**	**NO**
New School Google Apps	**OK** for working copies	**OK** for working copies	**NO**	**OK**	**NO**
Adobe Creative Cloud	**DISCOURAGED**	**NO**	**NO**	**OK**	**NO**
Internet-based file & information storage services *Dropbox, Box.net, Apple iCloud, Office 365, Evernote, etc.*	**DISCOURAGED**	**NO**	**NO**	**OK**	**OK**
Personal Google accounts	**DISCOURAGED**	**NO**	**NO**	**OK**	**OK**
Internet-based sync & backup services *Carbonite, Sugarsync, Mozy, Apple iCloud, etc.*	**DISCOURAGED**	**NO**	**NO**	**OK**	**OK**

Clear Desk Policy

The Clear Desk Policy applies to all papers and physical materials (CD-ROMs, USB flash drives, external hard drives, etc.) that contain New School information that is classified at either the Restricted or Confidential level.

1. All papers and physical materials that contain New School Restricted information **must** be put away and stored out of sight when not in use. The use of locking desk drawers or file cabinets is **recommended**, but not required.
2. All papers and physical materials that contain New School Confidential information **must** be put away and stored out of sight when not in use. The use of locking desk drawers or file cabinets, or locked file storage rooms/areas, is **required**.
3. Computer screens must be protected by a password-controlled screen saver or lock screen, or computers must be logged off, when not in use.

Safeguarding Mobile Devices

Laptops, tablets, and cell phones are easy to lose; they are also inviting targets for thieves. Follow these tips to keep information on these devices safe.

1. Secure cell phones and tables that are connected to New School email or New School Google Apps with a passcode or security pattern, and set the device to automatically lock after a few minutes (less than five) of inactivity.
2. Set up your phone's or tablet's "find me" function (Apple iCloud and Google Play both have this feature, as do several third-party apps).
3. Configure laptops to require a password at boot, at wake from hibernate, and at wake from sleep.
4. When not in use, keep laptops locked away. When in use, secure them to a permanent fixture using a locking cable.
5. Do not use your laptop (or laptop bag) to "hold your place" at the library, café, or elsewhere.
6. Report any loss or theft of a mobile device containing New School information to Campus Security and the IT Help Desk **immediately.**

Lock Your Computer Whenever You Leave Your Desk

Whenever you leave your desk—to go to lunch, attend a meeting, visit the restroom, or even just to pick up a printout—you should lock your computer so that passersby cannot see any sensitive information you might have on the screen, and nobody can access your files and email while you're gone.

Locking and Unlocking a Windows PC

Locking your PC doesn't require any special setup.

To Lock

1. Press **CTRL-ALT-DELETE** (hold down the CTRL and ALT keys and press the DELETE key)
2. Click "Lock This Computer" or just press **ENTER**

To Unlock

1. Press **CTRL-ALT-DELETE**
2. Enter your password and press **ENTER**

Locking and Unlocking a Mac

Before you can lock your Mac, you need to perform a few one-time setup steps:

4. If your Mac doesn't have a logon password, go to **System Preferences > Users and Groups**, select your account, and "change" (set) your password.
1. Go to **System Preferences > Security & Privacy > General**
2. Check the box next to **Require Password**
3. Set the interval to "**immediately** after sleep or screen saver begins"

To Lock

1. Press **CONTROL-SHIFT-EJECT** or, if your keyboard doesn't have an **EJECT** key, press **CONTROL-SHIFT-POWER**

To Unlock

1. Wiggle the mouse to turn the screen back on
2. Enter your password and press **ENTER**

Locking your computer will not interrupt your work, and when you unlock, you'll pick up right where you left off.

It takes a little getting used to, but soon you'll find that locking your screen whenever you leave your desk has become habit.

INFORMATION CLASSIFICATION AT THE NEW SCHOOL*

Unrestricted Information

Unrestricted information is information that can be disclosed to any person inside or outside the university. Although security controls are not needed to prevent disclosure and dissemination of this information, they are still necessary to protect against unauthorized modification, destruction, or loss of the information.

Examples

- Student information designated as public or directory information by The New School under the Family Educational Rights and Privacy Act (FERPA):
  - Student name
  - Major field of study
  - Dates of attendance
  - Full- or part-time enrollment status
  - Year level
  - Degrees and awards, including dean's list
  - Addresses
  - Telephone numbers
  - Photographs
  - E-mail addresses
  - Date and place of birth
  - Most recent previous educational agency or institution attended
- Faculty and staff directory information and any general biographical information already published by the faculty or staff member:
  - Employee name
  - Job/position title
  - Office mailing address
  - Office telephone number
  - Office e-mail address
  - Curriculum vitae
- General information about The New School:
  - Campus maps
  - Course catalogs and schedules
  - Campus brochures
  - Publications, blog entries, and message board postings
  - Student policies and handbooks
  - School calendars
  - Donor names, amounts, designations
  - Any item The New School has published in the past

Restricted Information

Restricted information is information that is generally not public, and whose disclosure, loss, or corruption may cause embarrassment or damage (financial or otherwise) to The New School. This information requires protection against unauthorized access and disclosure, modification, destruction, and use. However, the sensitivity of this information is less than that of Confidential information.

Examples

- Employee N-number
- Employee place of birth
- Employee home address
- Employee evaluations
- Employee resumes
- Individual employee salary data
- Individual employee benefit data
- Gender
- Individual student tuition payment information
- Internal correspondence and minutes from committee meetings that do not include Confidential information
- Class rosters
- Student grades
- Student resumes
- Student academic records
- Library transactions
- Vendor contracts
- Invoices and internal billing
- Detailed annual budget information
- Financial transactions that do not include Confidential data
- Internal operating procedures of the university that do not include Confidential information

Confidential Information

Confidential information is information whose disclosure, loss, or corruption would cause significant embarrassment or damage (financial or otherwise) to The New School or the individuals who are the subjects of the information. Confidential information includes any information that is protected under federal or state laws or regulations, personally identifiable information about faculty, staff, and students, and sensitive information about the university. This information requires a high level of protection against unauthorized access and disclosure, modification, destruction, and use.

Examples

- Student N-number
- Social Security number
- Driver's license number
- Other government-issued ID number
- SEVIS number
- Immigration status
- Disability or veteran status
- Protected Health Information (HIPAA)
- Ethnic, religious, racial, or national affiliation
- Human Resources information on individual applicants
- Donor information (except name, amount, designation)
- All anonymous donor information
- Directory information for students who have opted-out of public disclosure
- Employee date of birth
- Employee payroll information
- Employee disciplinary information
- Bank account numbers
- Credit/debit card numbers
- Wire transfer information
- Payment history information
- Individual taxation records
- Individual student counseling information
- Individual student disciplinary information
- Federal individual financial aid / grant information
- Privileged data in the Office of the General Counsel
- Information security data, including passwords and sensitive information related to the university's information technology infrastructure and operations

Handling Requirements

Highlights:

- Restricted and Confidential information **may not** be copied to:
  - Internet file storage sites (such as Adobe Creative Cloud, Apple iCloud, Microsoft SkyDrive, Google (except New School Google Apps), Box, Dropbox, SugarSync, etc.)
  - Cloud backup services (such as Mozy, Carbonite, Crash Plan, etc.)
  - Internet file sharing sites (such as YouSendIt, MediaFire, 4Shared, RapidShare, etc.)
  - Internet photo sharing sites (such as Flickr, Picasa, etc.)
- Confidential information **may not** be sent via email; use the Secure File Transfer Service (sendfiles). Restricted information may be sent to internal addresses via email but not outside the university; use of sendfiles is recommended. (Special rules apply to sending N-numbers via email; see detailed requirements).
- Restricted and Confidential information must be disposed of by placing them in secure, locked recycling bins designed for sensitive information or shredding them in a cross-cut shredder. Documents must not be placed in normal office trash cans or non-secure waste paper / recycling bins.

Detailed requirements for handling Restricted and Confidential information, in both electronic and non-electronic forms, are documented in ***General Controls for Handling Sensitive Information***, which can be found on the IT web site at: http://www.newschool.edu/informationtechnology/handling-sensitive-information.pdf.

* This information is excerpted from *The New School Information Security Policy*, Revision 1.0 (November 18, 2011)