Clear Desk & Clear Screen Policy

Purpose

This Policy establishes guidelines for maintaining a clear desk and clear screen to help protect University information (including student, research, financial, personnel, and operational information) from unauthorized access, loss, or disclosure, and to support compliance with applicable laws, regulations, contracts, and University policies.

Scope

This Policy applies to all University faculty and staff (including temporary and student employees), and contractors/consultants when using University workspaces or devices, or handling University information (collectively, "Users"). It applies to all physical records (paper), removable media, University-owned and personally owned devices used for University business, and all screens/displays that may present University information, whether in on-campus offices, labs, shared work areas, classrooms, meeting spaces, clinics, and libraries, and off-campus/remote work locations.

Definitions

- "University Information": Information created, received, maintained, or used for University business in any form (paper, electronic, and audio/visual), including information subject to FERPA, HIPAA, GLBA, research sponsor requirements, export controls, or other confidentiality obligations.

- "Sensitive Information": University Information that requires additional protection due to confidentiality, privacy, legal, contractual, ethical, or operational requirements (e.g., student records, patient records, personnel files, personally identifiable information, research data not intended for public release, financial account information, and authentication credentials).

- "Clear Desk": The practice of removing Sensitive Information and other high-risk items from desktops and work surfaces and securing them appropriately when not in use.

- "Clear Screen": The practice of preventing unauthorized viewing or access to Sensitive Information displayed on a screen, including by locking devices when unattended and taking steps to reduce inadvertent or deliberate viewing.

- "Unattended": A workspace or device that is not under the direct control of an authorized User (even briefly), including when stepping away for meetings, breaks, teaching, or leaving for the day.

Guidelines

Clear Desk (Paper Records And Physical Items)

- When leaving a workspace unattended (including stepping away briefly), Users should ensure Sensitive Information is not left in plain view. At a minimum, Sensitive Information should be placed in a locked drawer, locked filing cabinet, locked office, or other approved secure storage.

- At the end of each workday (or when departing a University workspace), desktops and work surfaces should be cleared of Sensitive Information, including notes, forms, grade rosters, advising notes, medical/clinical paperwork, financial records, and research materials that are not approved for public release.

- Keys, access cards, and physical tokens used to access restricted areas, cabinets, or secure information should not be left unattended on desks, in unlocked drawers, or in other accessible locations.

- Password lists, MFA backup codes, and other authentication secrets credentials **must never** be written on sticky notes or left in accessible locations.

- Sensitive Information should not be stored in open mail trays, on top of printers, or in public-facing reception or shared work areas unless continuously attended by an authorized User.

- Whiteboards, flip charts, and shared boards should be cleared of Sensitive Information when a meeting ends or when the space is vacated, unless the room is secured and access controlled.

Clear Screen (Workstations, Laptops, Tablets, Phones)

- Devices should be locked whenever unattended. Users should manually lock their screen before stepping away (e.g., for a meeting, classroom activity, or break).

- Where technically feasible, University-managed devices should be configured to automatically lock after a short period of inactivity. Users must not disable screen-lock or other required security controls.

- Monitors and screens displaying Sensitive Information should be positioned to reduce inadvertent viewing by others (e.g., visitors, students, vendors, and the public). Privacy screens should be used when appropriate.

- Sensitive Information should not be left visible on screens in public or semi-public spaces (e.g., classrooms, hallways, shared offices, and reception areas) unless necessary for business and continuously monitored by an authorized User.

- When teaching, presenting, or meeting, Users should take reasonable steps to avoid exposing Sensitive Information via projected screens, screen-sharing, or pop-up notifications.

Printing, Copying, Faxing, And Scanning

- Users should collect printouts containing Sensitive Information immediately, and should not leave them unattended on printers, copiers, or in output trays.
- Before printing Sensitive Information, Users should verify the correct device/location and ensure the printer is in a non-public area when possible.
- Where available, Users should use secure/locked printing features (badge/PIN release) for Sensitive Information.
- Misprints and unneeded copies containing Sensitive Information should be securely destroyed using approved shredders or confidential disposal bins; they should never be placed in regular trash or recycling.
- Scanned files containing Sensitive Information should be saved only to University-approved storage locations with appropriate access controls and should not be sent to personal email accounts or personal cloud storage.
- Faxing Sensitive Information should be avoided unless required for business reasons and should only be sent to verified recipients using secure procedures.

Storage Of Paper Records And Removable Media

- Paper records containing Sensitive Information should be stored in lockable storage (e.g., locked filing cabinets, locked desks, and locked offices) when not actively in use.
- Removable media (USB drives, external hard drives, and optical media) containing University Information should be handled as sensitive and should be physically secured when not in use. Where University policy permits removable media, it should be encrypted and approved for the intended use.
- Sensitive Information should not be left in vehicles, unattended bags, or other unsecured locations.

Meetings, Classrooms, Labs, And Shared Spaces

- Sensitive Information should not be left unattended in meeting rooms, classrooms, labs, or shared offices (including on desks, lecterns, podiums, lab benches, or conference tables).
- At the end of meetings/classes, Users should remove or secure handouts, sign-in sheets, grading materials, and meeting notes that contain Sensitive Information.

- Users should exercise discretion when discussing Sensitive Information in open areas, and verify that only authorized Users are present.

- When using shared computers or podium systems, Users should log out of applications and accounts at the end of use and ensure files are not saved locally on shared devices.

Remote Work, Home Offices, And Travel

- Sensitive Information should be protected from household members, guests, and others who are not authorized to access it.

- Users should not print Sensitive Information at home unless necessary for business and secure disposal (cross-cut shredder or approved confidential disposal process) is available.

- When traveling, Users should keep devices and paper records under physical control or secured (e.g., locked hotel safe where appropriate). Users should not leave University Information unattended in vehicles.

- Users should use privacy screens and be alert to inadvertent or deliberate viewing in public settings (airports, cafés, and conferences). Users should lock devices whenever not actively in use.

Visitors, Shared Access, And After-Hours Practices

- Visitors, vendors, and non-employees should not be left unsupervised in areas where Sensitive Information is visible or accessible.

- At the end of the day (and before weekends/holidays, vacations), Users should clear desks and secure Sensitive Information because cleaning, maintenance, security and other personnel may have after-hours access to facilities.

Enforcement and Disciplinary Action

Failure to comply with this Policy may result in disciplinary action, up to and including termination of employment, and may be referred for legal action if laws are violated. Reports of policy violations can be made to the Office of Human Resources or via the University's confidential compliance hotline.

Implementation And Oversight

The Office of Human Resources will oversee enforcement of this Policy. Questions or concerns should be directed to the Chief Human Resources Officer.

Any suspected or actual loss, theft, or unauthorized disclosure of Sensitive Information (paper or electronic) must be reported promptly to Information Security (infosec@yu.edu) in accordance with incident reporting procedures.

Related Policies

- Code of Conduct
- Data Classification Policy
- Employee Handbook
- Encryption Policy
- Information Security Policy
- IT Handbook
- ITS Policy for Handling Credit Card Information
- ITS Requirements for International Travelers
- Record Retention Policy
- Remote Work Policy

(March 2026)