Information Classification at The New School

Classification Levels
In increasing order of protection level, the classifications used by The New School are Unrestricted, Restricted, and Confidential.

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.

This information is excerpted from The New School Information Security Policy, Revision 2.0 (July 1, 2016).
Examples

- 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
- 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

- 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

- Information disclosed to or created by the University Ombuds
- 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

---

2 Prior to July 1, 2016, N-numbers belonging to employees were classified as Restricted and N-numbers belonging to students were classified as Confidential. To eliminate confusion, especially in cases where an individual is both a student (or former student) and an employee (or former employee), the classification of N-numbers belonging to employees has been changed so that, as of July 1, 2016, all N-numbers are classified as Confidential.
Assigning Classification Levels
Information Owners are responsible for assigning the appropriate classification to each information resource for which they are responsible, and ensuring that the resource is protected in accordance with that classification.

Many information resources will not be explicitly classified, particularly if they are not in the form of a printed or electronic document. Information that is not explicitly classified is classified implicitly as follows: Any information that contains confidential elements as defined above is classified as Confidential. Other information is classified as Restricted unless it is published (made publicly available in any medium) by the Information Owner, in which case it is classified as Unrestricted.

Handling Classified Information
The classification level determines the information security controls that must be applied to protect an information resource, and the procedures that must be followed when acquiring, storing, using, transmitting, archiving, and destroying that resource.

The Standard for Handling Sensitive Information describes the techniques and tools that should be used when:

- Providing (restricting) access to information
- Labeling information
- Storing electronic information
- Storing printed information
- Printing information
- Transmitting information
- Using classified information
- Archiving information (record retention)
- Disposing of (destroying) information

Non-Disclosure Agreements and Confidentiality Terms
Before Restricted or Confidential information may be disclosed to individuals or organizations outside The New School, including business partners, suppliers, and vendors, the Office of the General Counsel must be consulted to ensure that appropriate non-disclosure agreements or confidentiality contract terms are in place.