ETHICS BASED ON POLICIES
On TRACKING, SHARING, SECURITY DATA
IN HIGHER EDUCATION.
Focus on Teachers College.

Writers:
Shreya Goel
Fengxian Liu

Under Supervision of John Saul

Teachers College
Columbia University

December 14, 2017

CONTENT

SUMMARY

Scope*:* Applicable to all individuals who access, use or control Applicant/Student/Administrative Data at Teachers College, regardless of means or location of data storage, including faculty, staff and students, as well as project participants, contractors, consultants, volunteers, other agents of the College, individuals authorized to access Data and to those who supervise such individuals..

Data Ownership: "Teachers College owns all its Enterprise Data and system assets and is the Security Authority of data classified according to Teachers College Security Classifications".

Access and Confidentiality: Access to Data should be based on business needs of organization to achieve its mission. All requests to access data beyond the normal duties of employees must be addressed by Data Stewards.

Data Sharing Agreement: California state law on notice-triggering and Country specific data sharing agreements must be abided if and when needed.

Legal Issues: Refer/Consult Office of General Counsel (OGC), Teachers College for any legal issue/claim/demand/document or subpoena before responding to it.

Encrypt and/or Password Protect for the confidentiality of sensitive/confidential data, before transmission, during, but not limited to file transfers, emails, interactive sessions, web-based applications, network printer communications, remote file services, database access, application to application communications, virtual private network (VPN) connections; on portable computing devices, storage media, individual files stored over a network or offline storage devices and during backup or archival. Communication of decryption passwords must be made via different means such as telephone. Instructions for password protecting and encrypting can be found at http://www.columbia.edu/acis/security/articles/data/encryption.html

General Guideline for all Data Users:

- Do not redistribute sensitive/confidential data within or outside TC, unless you are an authorized distributor and the recipient is authorized receiver of data.
- Know and comply with the data classification being used at TC and follow the appropriate security measures listed for each category.
- Know and comply with the encryption guidelines.
- Never falsify your identity or enable others to falsify identity.
- Safeguard electronic access with strong passwords.
- Ensure that any computer used to access the resources/data, whether located on campus or elsewhere, is secure, virus-free, and otherwise not compromised.
- Create separate accounts for each person who uses the computer, setting appropriate permissions.
- Double check recipient's email before communicating any confidential/sensitive data.
- Scan for viruses and be cautious about opening email attachments at all times.

NOTE: This is just for a quick review and does not include details on all aspects related to Ethics to be followed in Higher Education. Please refer to the main document for detailed explanation and the list of references. Ethics for Student data, other administrative data may include more details which are not included here, but these ethics do apply to all types of data.

Scope of Ethics based on Policies

Employees

These ethics are applicable to all individuals who access, use or control Applicant/Student/Administrative Data at Teachers College, including faculty, staff and students, as well as project participants, contractors, consultants, volunteers, other agents of the College, individuals authorized to access Data (Teachers College, 2015) whose job responsibilities include inputting, safeguarding, retrieving, or using Data, and to those who supervise such individuals (NYU, 2017).

Data

These ethics are applicable to all Administrative Data related to applicants regardless of means or location of storage. Therefore, this applies to Source Data Systems and Administrative Data extracted from those Source Data Systems, as well as data stored in any data repository (NYU, 2017).

Access and Confidentiality

Access to Data should be based on business needs of organization only, to achieve its mission. Employees shall have access to data needed to perform their responsibilities (NYU, 2017). Requests to data access beyond the normal duties of employees must be addressed by Data Stewards assigned by the Provosts and VPFA at TC (Teachers College, 2015). Access to sensitive data should be granted only on an "as needed/minimum necessary" basis (NYU, 2017).

Each individual who has access to Data should know the data classification being used and should follow the appropriate security measures (NYU, 2017).

Data Classification

All those responsible for or working with the data should be aware of the following data classification scheme adopted by Teachers College:

Table 1: Data Classification Scheme

Data Category	Level of sensitivity	Definition	Examples
Sensitive Data	High	Information protected by federal, state or local laws and regulations or industry standards, such as FERPA, the New York State Information Security Breach and Notification Act, similar state laws and PCI-DSS or Personally Identifiable Information (PII) (Teachers College, 2015).	Name Date of Birth Place of birth - All geographic subdivisions smaller than a state (UC Berkeley) Mother's maiden name Biometric records Full face images (The University of Texas at Austin, 2015) Social security number Driver's license number or non-driver identification card number Email address with password (in certain narrow instances)

			Health/Medical information Educational information - Financial Aid Records (UC Berkeley) - Transcripts (UC Berkeley) Financial information - Account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account - Payment Card Industry (PCI) Information (UC Berkeley) Employment information
Confidential Data	Medium to High	Information considered appropriate for confidential treatment by Law/Contract/College (Teachers College, 2015).	Student education records. Non-public personal and financial data about donors. Citizen or immigrations status. Unpublished College financial information. Information on facilities security systems or system configurations related to information security. Nonpublic intellectual property, including invention disclosures and patent applications. Applicant financial information.
Internal Data	Low	Information proprietary /produced for the TC community only (Teachers College, 2015).	Internal operating procedures and operational manuals, Internal memoranda. Emails, reports and other documents. Technical documents such as system configurations and floor plans.
Public Data	None	Information that may/must be made available to the general public, with no legal restrictions on its access or use (Teachers College, 2015).	Statistical reports, fast facts (The University of Texas at Austin, 2015)

NOTE: If Data is found to be from more than one level of sensitivity in the same System or Endpoint, such Data shall be classified at the highest level of sensitivity.
References and notes on each column of Table 1:
Data Categories (Teachers College, 2015)
Level of sensitivity is predicted by Ethics formulation team.
Definitions (Teachers College, 2015)
Examples chosen from Teachers College, Data Classification and are not referenced in the table, in case the examples are from other resources, they are mentioned. The listed are examples that are included in each category but are not limited to these only.

Roles and Responsibilities

Data Ownership
"Teachers College is the owner of all its Enterprise Data and system assets and is the Security Authority of data classified according to Teachers College Security Classifications" (Teachers College, 2015).

The Provost and the Vice President for Finance and Administration (VPFA) responsibilities include, but are not limited to:

- Assigning Data Stewards.
- Ensuring that System Owners and Data Stewards receive proper training in handling confidential/sensitive data.
- Ensuring that System Owners and Data Stewards appropriately identify and classify Data in accordance with the TC Data Classification Policy (Teachers College, 2015).

Data Users: All data users should read, understand and comply with data policies and procedures of TC (Teachers College, 2015).

Data Stewards are College faculty and staff assigned by the Provost and the VPFA to coordinate with the CISO, the appropriate level of security for the data and systems under their control. IT Custodians must be informed, with the help of Data Classification Schema about the sensitivity of the data. **IT Custodian** with the CISO must then establish the appropriate security terms and conditions. Final implementation should be based on a risk assessment of the system and/or processes performed in conjunction with the CISO. Responsibilities of Data Stewards include (not limited to):

- Maintaining Data and integrity of the information.
- Managing data generation.
- Approving and Authorizing access privileges to Data and Systems.
- Confirming the stored information.
- Identifying and classifying Data in accordance with the TC Data Classification Policy.
- Labeling Sensitive Data and Confidential Data clearly, with support from the CISO.
- Establishing and implementing security requirements for such Data in consultation with the Director of Information Security.
- Ensuring information in all forms e.g. paper, cloud hosted data, and TC hosted data, is disposed of according to TC policy and procedure. (Teachers College, 2015).

Chief Information Security Officer (CISO) is responsible for the day to day management of the Data Security which includes but is not limited to:

- Work with departments, faculty and staff to keep them informed about the acceptable solution and to determine workable solutions.
- Educate and advise College personnel about data security.
- Collaborate with Data Stewards, Custodians, and System Owners to determine the appropriate means of using data.
- Consult and work with Office of general Counsel on legal and regulatory issues.
- Monitor communications and Data that use the College Network or Systems for transmission or storage.
- Conduct security assessments of Systems, and Data centers.
- Erase all Data stored on personal endpoints previously used for College business, as requested or required.

- Support the College's Emergency Response Team, led by the VPFA in connection with any breach or compromise of sensitive data, to the extent provided for in the Teachers College Electronic Data Security Breach Reporting and Response policy.

The College Director of Information Security is the Security Manager responsible as the Chief Information Security Officer (CISO). (Teachers College, 2015).

IT Custodians are College personnel or service providers who oversee the safe transport and storage of data, and establish and maintain the underlying infrastructure. (NYU, 2017; Teachers College, 2015).

Data Security

Definitions as adopted by TC

- **Confidentiality** means that information is only accessible to authorized users for authorized purposes (Teachers College, 2015).
- **Integrity** means safeguarding the accuracy and completeness of Data and processing methods (Teachers College, 2015).
- **Availability** means ensuring that authorized users have access to Data and associated Information Resources when required (Teachers College, 2015).

General Guideline for all Data Users:

- Know and comply with TC data classification scheme (Teachers College, 2015), encryption guidelines (Teachers College, 2017), university rules, federal laws and state laws (Teachers College, 2017), The University of Texas at Austin, 2015; NYU, 2017).
- Protect all data for confidentiality, integrity and availability from improper or unauthorized use, including such use by third parties, regardless of the storage medium (e.g., paper, fiche, electronic tape, cartridge, disk, CD, DVD, external drive, copier hard drive, cloud-based storage, computers) and regardless of form (e.g., text, graphic, video, audio) (NYU, 2017; Teachers College, 2017).
- Control for unauthorized use of university data, information, resources, systems (The University of Texas at Austin, 2015).
- Never falsify your identity or enable others to falsify identity (Teachers College, 2017; The University of Texas at Austin, 2015).
- Safeguard electronic access with strong passwords (The University of Texas at Austin, 2015).

Safeguarding Data: Protecting sensitive/confidential data:

<u>Computers</u>

- Know what data are stored on your computer and the level of sensitivity of that data. (NYU, 2017).
- Ensure that any computer used to access the resources/data, whether located on campus or elsewhere, is secure, virus-free, and otherwise not compromised (NYU, 2017).
- Refrain from activities that interfere with the ability of others to use computer and data resources (NYU, 2017).

<u>In case of shared computers</u>

- Safeguard sensitive/confidential data that others may not be authorized to access (NYU, 2017).
- Create separate accounts for each person who uses the computer, setting appropriate permissions (NYU, 2017).

<u>Data storage</u>

- Whole Disk Encryption: Portable computing devices (e.g., PDAs, tablet PCs, laptops, and smartphones), storage media, (e.g., CDs, DVDs, and USB drives) (The University of Texas at Austin, 2011).

- File Encrypting: Individual files to be stored over a network or to offline storage devices (e.g., CDs, DVDs, or USB drives) (The University of Texas at Austin, 2011).
- Database Storage - Password protect or encrypt sensitive/confidential data, where possible (NYU, 2017; The University of Texas at Austin, 2011).

Backup and Archiving

- Encrypt sensitive/confidential data for Backup and Archiving (The University of Texas at Austin, 2011).
- Backup local data on a regular basis and keep the backup secure. (NYU, 2017)
- Protect backups with the same level of security as the original data. (NYU, 2017)
- Test backup recovery periodically to verify that it works. (NYU, 2017)

Communication/Transmission

- Do not redistribute sensitive/confidential data within or outside TC, unless you are an authorized distributor and the recipient is authorized to receive that data. (NYU, 2017)
- Store sensitive data only on University servers, unless storage is authorized. (NYU, 2017;, The University of Chicago)
- Encrypt sensitive/confidential data before transmission, during, but not limited to file transfers, emails, interactive sessions, web-based applications, network printer communications, remote file services, database access, application to application communications, virtual private network (VPN) connections (The University of Texas at Austin, 2011).
- Use only TC emails for conducting college business and stay updated with email communications (Teachers College, 2017).
- Keep all emails sent or received as confidential as possible (Teachers College, 2017). Password protect or Encrypt any sensitive/confidential information (e.g., SSN, credit card, grades, medical information) sent by email (NYU, 2017; Teachers College, 2017; The University of Chicago). Never type such information in the body of the emails. Communication of decryption passwords must be made via different means such as telephone. Instructions for password protecting and encrypting MS Office documents can be found at http://www.columbia.edu/acis/security/articles/data/encryption.html (Teachers College, 2017).
- Double check recipient's email before communicating any confidential/sensitive data (NYU, 2017; Teachers College, 201; The University of Chicago).
- Scan for viruses and be cautious about opening email attachments at all times. (The University of Chicago)
- Do not transmit sensitive data using instant messaging technology such as Slack, WhatsApp, and Facebook Messenger (NYU, 2017).
- Mark any fax as confidential that contains sensitive/confidential data (NYU, 2017).
- Faxes, printouts, and copies of sensitive data should be picked up promptly and handled appropriately (NYU, 2017).
- Keep fax machines, printers, and copiers used for sensitive/confidential data in secure areas (NYU, 2017).

Disposal

- Destroy sensitive/confidential data in a manner that prevents re-creation. (NYU, 2017)
- Reformat/Physically destroy any removable storage media (such as floppy disks, zip disks, tapes, or compact disks (CD)) that contained sensitive data before disposing them. (NYU, 2017)
- Shred printouts of sensitive/confidential data. (NYU, 2017)
- Ensure that sensitive/confidential data are removed from devices you use, including remote printers, before you dispose of or redeploy those devices. (NYU, 2017)

Data Sharing

Definition of Student Under FERPA

Under Family Educational Rights and Privacy Act ("FERPA") policy, "students" are individuals who are or were registered students in attendance at Teachers College. Persons who unsuccessfully applied for admission or who were accepted but never attended the College are not "students." An unsuccessful applicant for admission to the College is not a College "student," even if the applicant is or was in attendance at another Columbia University school (Teachers College, 2017).

Circumstances under which Data containing PII can be disclosed

Under FERPA, records containing PII may be disclosed without consent to:

- To "**School Officials**" (A person employed by the College in administrative, supervisory, academic, research, or support staff position; public safety officials, members of the Board of Trustees; or a student serving on an official committee, such as a disciplinary or grievance committee or admission committee, or assisting another School Official in performing his/her tasks for the College) (Teachers College, 2017).
- To a **contractor** (School official) who performs an institutional service or function, under the direct control of the school such as an attorney, auditor or collection agent (Teachers College, 2017).
- In **connection with financial aid** for which the student has applied or received, to determine eligibility for aid, the amount of aid, or the conditions of aid; or to enforce the terms and conditions of aid (Teachers College, 2017).
- To **authorized representatives** of the U.S. Controller General, Attorney General, or Secretary of Education, to State and local educational authorities or to entities authorized by these representatives on their behalf. Disclosures under this provision may be made, subject to the FERPA requirements (Teachers College, 2017).
- To **organizations conducting studies for, or on behalf of**, the college,in order to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs: or (c) improve instruction (Teachers College, 2017).
- To **comply with a judicial order** or lawfully issued subpoena (Teachers College, 2017).
- To officials in connection with **health/medical emergency** subject to provisions of the regulation (Teachers College, 2017).
- To **parents** of a student under the age of 21 regarding student's violation of any Federal, State or local law or of the school (Teachers College, 2017; The University of Chicago, 2017).

Data Sharing Agreement

Data-Sharing Agreement and its Importance (The University of Chicago, 2011)

A data-sharing agreement is a formal contract that clearly documents what data are being shared and how the data can be used. Before any data are shared, both the provider and receiver should communicate discuss data-sharing and data-use agreement which serves the following purposes:

- Protects the agency providing the data.
- Ensures that the data will not be misused.
- Prevents miscommunication on the part of the provider of the data and the agency receiving the data
- It makes certain that any questions about data use are discussed.

California State Law Notice-Triggering Information (UC Berkeley)

"California law requires a business or a state agency to notify any California resident whose unencrypted personal information, as defined below, is accessed by an unauthorized person".

This information may include but is not limited to individual's first name or initial and last name plus Social Security Number, Driver's license number or California Identification Card number, Account number, credit or debit card number, in combination with any required security code, access code, or password that would, Medical Information, Health Insurance Information.

Country specific data sharing agreements must be abided if and when needed. (The University of Chicago, 2011)

Legal Issues and Ethics

Based on Office of General Counsel (OGC) Teachers College Policies/Guidelines on Acceptance of legal documents-

Scope of Legal Issues (Teachers College)

- TC related
- Legal notice
- Legal demand
- Legal claim
- Legal dispute
- Complaint, Petitions, Other legal documents
- Subpoena in connection with matter involving TC
- Subpoena received in mail by any college employee, staff, faculty, student

Ethics/Guidelines

- Teachers College; all college departments and units, employees, staff members, faculty members, students should refer/consult/contact **OGC** immediately for any/all of the above mentioned Legal issues before accepting/responding to them at all times (Teachers College).
- Any documents related to legal claims should be delivered to the OGC with immediate notification to OGC (Teachers College).
- All records must be maintained in terms of who is the recipient, how was it delivered (by mail/email/messenger/in person) and where was the legal notice/claim delivered and forwarded (Teachers College).
- If a college Employee, Staff, Faculty, Student receives a subpoena by mail, OGC should be notified immediately, to validate the subpoena and respond appropriately (Teachers College).

NOTE: Legal Issues and Ethics are not limited to applicant data and can be applied to other circumstances and situations as well.

References

NYU (2017, January 27). Administrative Data Management Policies. Retrieved from https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/administrative-data-management-policy.html

NYU (2016, October 3). Data Classification Table. Retrieved from https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/data-classification.html

NYU (2017, April 19). Policy on Responsible Use of NYU Computers and Data. Retrieved from http://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/responsible-use-of-nyu-computers-and-data-policy-on.html

Teachers College. Acceptance of Legal document. Retrieved from http://www.tc.columbia.edu/policylibrary/general-counsel-/acceptance-of-legal-documents-/

Teachers College (2015, April). Data Classification. Retrieved from http://www.tc.columbia.edu/policylibrary/computing-and-information-services/data-classification-/

Teachers College (2017, December). Email Us . Retrieved from http://www.tc.columbia.edu/policylibrary/Email Use

Teachers College (2015, January).Information Security Charter. Retrieved from http://www.tc.columbia.edu/policylibrary/computing-and-information-services/information-security-charter/

Teachers College (2017, September). Student Records and Family Education Rights and Privacy Act (FERPA) Statement. Retrieved from http://www.tc.columbia.edu/policylibrary/associate-provost-enrollment-services/student-records-and-family-education-rights-and-privacy-act-ferpa-statement/

The University of Chicago (2011, April 11). Data-Sharing Agreement. Retrieved from https://ura.uchicago.edu/page/data-sharing-agreements

The University of Chicago (2017, July 14). Legal: Privacy Policy. Retrieved from https://collegeadmissions.uchicago.edu/legal-privacy

The University of Chicago. UChicago Guide to Sensitive Data Usage. Retrieved from http://dataguide.uchicago.edu/

The University of Texas at Austin (2015, August 24). Acceptable Use Policy for University Students. Retrieved from https://security.utexas.edu/policies/aup

The University of Texas at Austin (2015, September 24). Data Classification Standard. Retrieved from https://security.utexas.edu/policies/data_classification

The University of Texas at Austin (2011, March 3). Data Encryption Guidelines. Retrieved from https://security.utexas.edu/policies/encryption

UC Berkeley. Data Use Agreement. Retrieved from https://security.berkeley.edu/uc-berkeley-box-and-google-data-use-agreement