BARNARD
BARNARD COLLEGE • COLUMBIA UNIVERSITY

Barnard College Policy on Handling Sensitive Information and Our Duty of Confidentiality

Effective Date: May 4, 2021

Executive Summary:

Access to Barnard College data, information, systems, and applications is based on your need for access and your agreement to use this access appropriately. Therefore, before you can be granted access, you must read and agree to follow Barnard's Acceptable Use Policy and you must accept responsibility to preserve the security and confidentiality of information that you access, in any form, including oral, print, or electronic formats.

Reason for this Policy:

Information, of various types and in various forms, are integral resources that support the education, research and service missions and operations of the college. Inappropriate use of these resources threatens the atmosphere for the sharing of information, the free exchange of ideas, and a secure environment for creating and maintaining college resources. In addition, there are laws, regulations, and institutional policies that govern how we must protect the information that we, as members of the Barnard Community, come in contact with as part of our daily operations.

Who is Responsible for This Policy:

Responsible Administrators: Executive Director for Human Resources
Executive Director for Information Technology

Responsible Office: Barnard College Information Technology (BCIT)

Who is Governed by This Policy:

This policy applies to all individuals who access, use, or control Sensitive Information on behalf of Barnard College. Those individuals include, but are not limited to, staff, faculty, students, those working on behalf of the College, and individuals authorized by affiliated institutions and organizations.

Please be aware that managers of certain services or information types may require you to adhere to additional standards and/or complete additional agreements and/or training.

You will be asked to periodically refresh your knowledge of the expectations to protect sensitive information that you come in contact with during your role and responsibilities with Barnard College.

Definitions:

Confidentiality: A duty of confidentiality means that information is protected from unintentional, unlawful, or unauthorized access, disclosure, or theft. Sensitive Information should only be disclosed to authorized individuals, entities, or processes.

Institutional Systems: Applications, designated storage locations, and "systems of record" under the direct management of Barnard College. Examples include Colleague, PowerFAIDs, Workday, Canvas, Point and Click, SalesForce, Google Drive, and N drive.

Personally Identifiable Information: Nonpublic information relating to an individual that reasonably identifies the individual and, if compromised, could cause significant harm to that individual or to the college. Examples may include, but are not limited to, Social Security numbers, credit card numbers, bank account information, student grades or disciplinary information, salary or employee performance, donations, income statements, dates of birth, patient health information, information that the College has agreed to keep confidential, and account passwords or encryption keys used to protect access to confidential college data.

Proprietary Information: Data, information, or intellectual property in which the College has an exclusive legal interest or ownership right, which, if compromised, could cause significant harm to the college. Examples may include, but are not limited to, business planning information, financial information, trade secrets, copyrighted material, research or comparable materials from a third party that the College has agreed to keep confidential.

Sensitive Information: Any information whose unauthorized disclosure could cause harm to the College or its constituents including Personally Identifiable Information about staff, faculty, students, alumnae, families, donors, vendors and trustees, as well as any other information otherwise marked or known to be Confidential or Proprietary, such as academic research and non-public information. Other sensitive information may include third party information shared with Barnard College that is governed by a contractual relationship.

Policy Statement:

Sensitive Information, in any form, including oral, print, or electronic formats, must remain confidential and must be safeguarded from unauthorized disclosure, modification, or disruption by following Barnard's approved policies and procedures.

Use of and access to Sensitive Information is strictly limited to the scope of defined Barnard roles and duties. Departments may request execution of a Duty of Confidentiality Acknowledgement pertinent to specific types of Sensitive Information or responsibilities.

Everyone has an obligation to report misuse or unauthorized disclosure of Sensitive Information to the BCIT Service Desk, the data owner, or the Office of General Council. Such reporting is subject to the considerations defined within Barnard's Whistleblower Policy.

Standards for Secure Usage:

When handling Sensitive Information, you agree to the following:

- Never use your Barnard username and password combination for external services outside of Institutional Systems unless required by the provider because of its relationship with the College. Select strong passwords and avoid reuse of the same password across multiple accounts.
- Never share your passwords or access credentials with anyone. Change your password immediately if you know or suspect that your password has been compromised.
- Be mindful that different computer systems and applications provide different levels of protection for information. Seek advice from BCIT on supplemental security measures, if necessary.
- Use extreme caution when storing Sensitive Information outside of Institutional Systems or on mobile storage devices (e.g., laptops, USB drives, mobile phones, tablets, etc.) without proper protections approved. If persistent, regular storage is necessary for the operation of the department, please consult BCIT, Director, Information Security for appropriate guidance.
- Respect the College's information and system security procedures (i.e., never attempt to circumvent or "go around" security processes).
- Maintain Sensitive Information in a secure manner to prevent access, viewing, or printing by unauthorized individuals.
- Do not leave Sensitive Information in publicly or openly accessible locations, such as classrooms, meeting rooms, shared printers, or on publicly visible white boards or displays.
- Secure unattended devices (e.g., log off, lock, or otherwise make inaccessible), even if you will only be away from the computer or device for a short time.
- Store Sensitive Information securely (e.g., on secure servers, in locked file cabinets, etc.).
- When sending or providing Sensitive Information to authorized individuals outside of institutional systems, make sure that such information is sent to the correct recipient. If sent via electronic means, make sure appropriate encryption or other protective methods are used.

- All personal health information (PHI) collected on behalf of the College to support College business must be stored securely and de-identified where possible, whenever PHI is stored on electronic devices or transmitted outside of Institutional Systems.
- Securely dispose of Sensitive Information when no longer needed (e.g., by shredding, disk wiping, physical destruction, etc.).

Standards of Legal Usage:

The College's resources should be used in compliance with all Barnard policies, procedures, applicable local, state, federal and international laws and regulations.

You agree to:

- Use information and resources for legal and authorized purposes only.
- Respect and comply with all copyrights and license agreements.
- Never use your access to information or devices to harass, libel, or defame others.
- Never damage or reverse engineer equipment, software, or data belonging to others without explicit permission of the owner.
- Never make unauthorized use of computer accounts, access codes, or devices.
- Never monitor or disrupt the communications of others, except in the legitimate scope of your assigned duties.
- Abide by applicable laws and policies with respect to access, use, disclosure, and/or disposal of Sensitive Information. Applicable law and policies include, but are not limited to:
    - Family Educational Rights and Privacy Act (FERPA)
    - General Data Privacy Regulation (GDPR)
    - Health Insurance Portability and Accountability Act (HIPAA)
    - Protection of Human Subjects (45 CFR 46)

Standards of Ethical Usage:

The College's resources should be used responsibly, ethically, and professionally while maintaining consistency with the mission of the College.

- Access institutional information only in the conduct of business and in ways consistent with furthering the mission of education, research, and public service.
- Use only the information needed to perform assigned or authorized duties.
- Never access or use any institutional information to satisfy your personal curiosity.
- Use information and technology resources in ways that foster the high ethical standards of the College.
- Never use information or technology resources to engage in academic, personal, or research misconduct.

- Never access or use institutional information (including public directory information) for your own personal gain or profit, or the personal gain or profit of others, without appropriate authorization.
- Respect the confidentiality and privacy of individuals whose records you may access.
- Preserve and protect the confidentiality of all Sensitive Information as a matter of ongoing responsibility.
- Never disclose Sensitive Information or distribute such data to a third party in any medium (including oral, paper, or electronic) without a contract processed through or waived by the Office of General Counsel.

Reporting Procedure:
Any potential compromise of Sensitive Information through unauthorized access, loss, theft or other means, including any such Information stored on personal devices, must be immediately reported to the BCIT Service Desk (help@barnard.edu or 212-854-7172).

Enforcement:
Violations of this policy are adjudicated according to the procedures defined in the student, faculty, or employee policies and procedures and may result in the removal of access to Sensitive Information and/or more serious sanctions. The College also reserves the right to initiate criminal/civil prosecution, depending on the severity of the violation.

Related Policies and Documents:
For departments that require a specific acknowledgement for the handling of sensitive information and the associated Duty of Confidentiality, please use the ***Duty of Confidentiality Acknowledgment template*** https://portal.barnard.edu/sites/default/files/2021-10/Duty%20of%20Confidentiality%20Acknowledgment%20Template.pdf. This template can be customized with specific departmental data, roles, and the like, as needed so long as the fundamental statements remain.

Use of College resources are subject to many laws and regulations. Suspected violations of applicable law are subject to investigation by the college and possibly law enforcement officials.

Some of the applicable laws and regulations are as follows:

Family Education Rights and Privacy Act (FERPA): a federal law that protects the privacy of student education records.

Federal Copyright Law: U.S. copyright law grants authors certain exclusive rights of reproduction, adaptation, distribution, performance, display, attribution and integrity to

their creations, including works of literature, photographs, music, software, film and video. Violations of copyright laws include, but are not limited to, the making of unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recordings) and distributing copyrighted materials over computer networks or through other means.

Federal Computer Fraud and Abuse Law: Federal law prohibits unauthorized access to, or modification of information in computers containing national defense, banking, or financial information.

General Data Privacy Regulation (GDPR): a European Union (EU) data privacy regulation, effective May 25, 2018, protecting the personal data of EU subjects or others physically located in the EU which is collected by the college.

New York State "Stop Hacks and Improve Electronic Data Security Act" (SHIELD Act) : New York State legislation, effective March 2020, that requires employers in possession of New York residents' private information to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information.

New York Social Security Number Protection Law: A New York State legislation placing limits on the use and dissemination of social security account numbers.

Payment Card Industry Data Security Standard (PCI DSS): A set of requirements designed to ensure the protection of payment card data.

Defamation: Someone may seek civil remedies if they can show that they were clearly identified as the subject of defamatory messages and suffered damages as a consequence. Truth is a defense against charges of defamation.

Common law actions for invasion of privacy: Someone may seek civil remedies for invasion of privacy on several grounds.

Public disclosure of private facts: the widespread disclosure of facts about a person, even when true, may be deemed harmful enough to justify a lawsuit.

False light: a person wrongfully attributes views or characteristics to another person in ways that damage that person's reputation.

Wrongful intrusion: the law often protects those areas of a person's life in which they can reasonably expect they will not be intruded upon.

The following College Policies are referenced or applicable:

Acceptable Use Policy
Data Access Policy
Data Privacy Policy
Digital Copyright Compliance Information
Policy and Guidelines Regarding Student Records Under the Family Educational Rights and Privacy Act of 1974 (FERPA)
Whistleblower Policy

Website for This Policy: https://my.barnard.edu/BC%20Policies/Confidentiality%20Policy.pdf

Revision History:
June 15, 2020: Initial release