New York University
UNIVERSITY POLICIES

Title: University Access to Personal Digital Content
Effective Date: December 15, 2016
Supersedes: New Policy
Date of Latest Revision: N/A
Issuing Authority: Executive Vice President
Responsible Officer: Vice President, Information Technology and Chief Information Officer

Policy

It is the policy of New York University, including its Schools and other units, global locations, and all University Affiliates (together “NYU”), that NYU limits the circumstances under which NYU will access, disseminate, and use Personal Digital Content, or “PDC” (as defined in this policy) of NYU faculty, students, and staff, and that NYU be transparent about those circumstances and its related procedures.

NYU recognizes that as faculty, students, and staff increasingly create, receive, use, transmit, and store information in digital form — as opposed to traditional media (e.g., print materials, file cabinets) — there is growing concern that such information may be more vulnerable to unintended or inappropriate use. At the same time, NYU appreciates and affirms that NYU faculty, students, and staff have an expectation of privacy. Such privacy is a necessary part of fulfilling NYU’s commitment to academic freedom (as set forth in the Faculty Handbook), and its commitment to respect in its relationships with faculty, students, and staff (as set forth in the New York University Code of Ethical Conduct).

Purpose of this Policy

The purpose of this policy is to establish internal standards and procedures governing NYU’s access to, and dissemination and use of, PDC to achieve the above-stated policy objectives. This policy is grounded on six important principles:

- Access to, and dissemination and use of, PDC of NYU faculty, students, and staff will be authorized only by the PDC Access Panel, and access will be conducted pursuant to NYU’s Policy on Requests to Information Technology (NYU IT) to Support Investigations.
- Access to, and dissemination and use of, PDC of NYU faculty, students, and staff will occur only for a legitimate NYU purpose, as set forth in this policy.
- Except as provided in this policy notice pursuant to the Notice section of this policy will be given to affected NYU faculty, students, and/or staff when their PDC will be, or has been, accessed.
- Access to, and dissemination and use of, PDC of NYU faculty, students, and staff will be limited in scope to the information needed to accomplish the purpose.
- NYU will maintain sufficient records to enable appropriate review of compliance with this policy.
• Access to, and dissemination and use of, PDC will be subject to ongoing, independent oversight by an NYU Committee that will issue regular reports to the University Senate.

This policy does not create rights in any individual or entity to seek legal redress for action inconsistent with the policy.

Scope of this Policy

This policy affords protections to faculty, students, and staff of NYU with respect to their Personal Digital Content and sets forth NYU’s commitment and processes to effectuate those protections.

Procedures for Implementation

Background

NYU faculty, students, and staff rely on technology in multiple aspects of their work, teaching, research, study, and other activities. In doing so, they often use electronic systems, networks, and devices that NYU owns, provides, or administers. These NYU Systems assist NYU in carrying out certain activities. As used in this policy, “NYU Systems” means all information technology services, networks, and devices owned, provided, or administered by any unit of NYU. Services include, but are not limited to, email services, internet access, file servers, voice message servers, hardware and cloud-based storage devices and/or services, laptop, tablet, desktop, and other computers, phones or other mobile devices, and other outsourced information technology services (e.g., Google NYU Mail or Google Apps for Education).

This policy provides protections to NYU faculty, students, and staff with respect to their “Personal Digital Content” or “PDC,” which means the following content and its associated metadata to the extent stored in files and/or accounts on, or transmitted through, NYU Systems and that are associated with a specific NYU faculty member, student, or staff member:

(a) digital documents and communications of NYU faculty, students, and staff, such as emails, voice mails, text messages, audio and video files;
(b) internet search records and internet sites visited for specific NYU faculty, students, or staff;
(c) manuscripts and other similar works of authorship by NYU faculty, students, or staff that are not publicly available; and
(d) other scholarly content of NYU faculty, students, and staff that comprises “Traditional Works of Scholarship” under NYU’s Statement of Policy on Intellectual Property, except to the extent such works also qualify as “Instructional Media” under that policy.

Examples of content that are not included within the definition of PDC include: (a) logs or records of access, including video files, to NYU facilities or equipment; (b) “Research Data” as defined in NYU’s Policy on Retention of and Access to Research Data; (c) personal information needed for management of NYU records, such as financial, human resource, and student information system records; and (d) routine uses of NYU instructional management systems (e.g., the statistics section of NYU Classes). If members of the University community have a question about whether specific data is included within the definition of PDC, they should consult with their Dean or Director who, together with the Responsible Officer for this policy, will provide guidance.
Reasons for Access

NYU does not monitor the PDC of a specific NYU faculty member, student, or staff member. However, NYU may obtain access to such PDC in some circumstances, but only for a legitimate institutional purpose, as set forth in this policy. The paragraphs below describe certain purposes for which NYU may access such information. While this list is expected to cover most instances of access, the list is not intended to be exhaustive. NYU may access the PDC of NYU faculty, students, and staff for other comparable reasons that advance a legitimate institutional purpose, as determined pursuant to this policy and subject to review by the Oversight Committee as described below. In evaluating the institutional purpose, the PDC Access Panel will in each case weigh not only the stated reasons for access but also the possible effect of access on NYU values such as academic freedom and internal trust and confidence.

A. System Protection, Maintenance, and Management

NYU Systems require ongoing management, maintenance and inspection to ensure that they are operating properly; to implement new systems; to protect against threats such as attacks, malware, and viruses; and to protect the integrity and security of information. For example, system logs, also known as log files, are created during system operation and contain information about system events that are needed for specific business reasons or to satisfy legal requirements. Business reasons include, but are not limited to, deploying new software, troubleshooting, system testing, collecting metrics on system performance and usage, billing, documentation, electronic discovery, and forensic investigation. No routine network scans of faculty, students, or staff are done that examine content.

B. Business Continuity

NYU may access PDC of NYU faculty, students, and staff for the limited purpose of ensuring continuity in its business operations where the information in question is material to conducting business operations, and where it is reasonably determined that there is no better practicable alternative under the circumstances. This need can arise, for example, if an employee who typically has access to the files or business information in question is unavailable for the time period when the files or information is needed. The term “business continuity” includes University business and administrative data and files, but does not include teaching materials, scholarly works, or other similar academic information.

C. Safety Matters

NYU may access PDC of NYU faculty, students, and staff to deal with exigent situations presenting a threat to campus safety or the life, health, or safety of any person.

D. Legal and Regulatory Process and Litigation

NYU may access PDC of NYU faculty, students, and staff in connection with pending litigation or a bona fide threat of litigation (as determined by the Office of General Counsel), and to respond to subpoenas and similar lawful requests for information in relevant law enforcement investigations, other government investigations and regulatory processes, and legal and regulatory processes, and as otherwise required by law.

E. Internal Investigations and Audits
NYU may access PDC of NYU faculty, students, and staff: a) in connection with investigations under, and consistent with the requirements of, any applicable NYU policies (such as, for example, claims of discrimination, harassment, sexual misconduct, research misconduct, financial misconduct); b) for purposes of internal audits and audits by NYU’s public accounting firm; and c) in connection with claims relating to public safety, including allegations of criminal conduct, and other circumstances as outlined in policies such as Electronic Communications and Social Media, Missing Student Notification, Appropriate Use of Email at New York University, and Terms of Use for NYU Google Apps for Education. Access may be authorized only when the PDC Access Panel has determined that the investigation advances a legitimate institutional purpose and that there is a sufficient basis for it.

Authorization of Access

Access to PDC of NYU faculty, students, and staff must be authorized by a three-person standing University panel (“PDC Access Panel”) comprising the VP/CIO or his/her designee, a representative of the Office of General Counsel, and the Provost or his/her designee. The PDC Access Panel will develop and approve protocols for approvals. Once authorized by the PDC Access Panel, the VP/CIO or his/her designee will undertake access in accordance with NYU’s Policy on Requests to NYU Information Technology (NYU IT) to Support Investigations.

Any authorization of access by the PDC Access Panel will apply only to the particular situation and specific NYU faculty, students, and/or staff. Any other situation must be separately authorized.

No independent authorization is required for information technology personnel to conduct routine system protection, maintenance, or management in accord with internal protocols and processes. Likewise, requests for access in connection with litigation, legal and regulatory processes, or requirements, or law enforcement investigations, or to preserve PDC for possible subsequent access in accordance with this policy, need no independent authorization if made by the Office of General Counsel.

In exigent situations involving a threat to campus safety or the life, health, or safety of any person where there is no other governing policy, access may be authorized by the Office of General Counsel. If emergency conditions do not allow for prior authorization, the matter will be reported to the Office of General Counsel as promptly as possible.

Notice of Access

When NYU intends to access PDC of current NYU faculty, staff, and students, and except as otherwise provided in this policy, all reasonable efforts will be made to give notice to the affected community member(s) at or before the time of access or, where it is deemed necessary by the PDC Access Panel (e.g., to preserve the integrity of the PDC) as soon thereafter as reasonably possible, and consistent with any applicable laws and university policies. Notice will be provided by the VP/CIO and will ordinarily include a summary of the actions taken (including date and time of access), and the reasons the action was taken. However, the timing, content and scope of notice are often dependent upon unique circumstances, and the PDC Access Panel will establish for the VP/CIO any specific requirements for notice in each situation for which access has been authorized consistent with this policy.

The following are examples of situations where notice is not required:
A. System protection, maintenance, and management — Individual notice is not required for ordinary system protection, maintenance, or management as described in this policy. Notice should be given if the access relates specifically to the activity of an individual faculty member, student, or staff member, unless troubleshooting the individual user’s problem with a system based on a report from the user.

B. Business continuity — Individual notice prior to access normally is not required for access to PDC for purposes of business continuity, in accordance with this policy and established NYU practice, and the common understanding is that individual notice prior to access in such cases typically is not practicable.

C. Legal restrictions — Individual notice is not required where NYU is subject to legal constraints, or with requests by law enforcement or regulators, or similar constraints on NYU’s ability to give notice.

D. Emergencies and other extraordinary cases — Contemporaneous individual notice is not required in cases where there is insufficient time, where giving notice could otherwise interfere with an effective response to an emergency or other compelling need (e.g., at a stage of an internal investigation where giving notice could compromise the investigation, or in exigent situations presenting a threat to campus safety, or the life, health, or safety of any person), or where it is impracticable. The decision not to give contemporaneous notice to an NYU faculty member, student or staff member must be made by the PDC Access Panel. In such cases, notice will ordinarily be given as soon as practical.

E. Policy Restrictions – Notice is not required where providing such notice would be in violation of any other applicable University policies

The PDC Access Panel may decide not to give notice. Any such decision, and the grounds for overcoming the presumption set forth in this policy, will be documented, and available for review by the Oversight Committee, as set forth in this policy.

Scope of Access

NYU will adopt reasonable steps, whenever practicable, to limit access, dissemination, and use of PDC of NYU faculty, students, and staff obtained under this policy to the content that is related to NYU’s documented purpose in obtaining access. These steps will vary depending on the circumstances of the search. Participation in the search, and access to, and dissemination and use of, the PDC in question should be limited to those personnel with a reasonable need to be involved. To the extent un-encryption of any such PDC may be required, the protocols for un-encryption are legal in nature and beyond the scope of this policy.

Records of Process

The PDC Access Panel will ensure that reasonable records of the process are preserved, including who requested the access, the purpose for which the access was requested, who undertook any investigation, the process undertaken, and any decision reached. The PDC Access Panel will also ensure that any person involved in accessing PDC signs an acknowledgement that all such PDC will be held in strict confidence in accordance with this policy.
In all instances of access under this policy, records should be maintained that are adequate to permit effective review as described in the Oversight Committee section of this policy. Records will be maintained for a period of time that is consistent with all legal obligations and with custom and practice.

**Compliance with Laws**

There are numerous international, federal and state laws related to data privacy, data security, and data transfer. This policy should be understood in light of those laws, including the Family Educational Rights and Privacy Act of 1974, the Electronic Communications Decency Act of 1986, the Health Insurance Portability and Accountability Act of 1996, and implementing regulations.

**Oversight Committee**

This policy, its implementation and protocols, and instances of access under this policy will be subject to review by an Oversight Committee to be constituted by the Provost annually, which will include representatives (or their designees) from each council of the University Senate and appropriate senior administrators. The Oversight Committee will be provided at least annually with a report by NYU IT that categorizes the number of incidents where PDC of NYU faculty, students, and staff was accessed, and for each incident, the date of access, position of the individual(s) whose data was accessed (i.e., faculty, student, staff), the academic or administrative unit that requested access, the purpose for the access, whether there was notice provided, and whether such access, dissemination and use was in compliance with this policy and with NYU’s Policy on Requests to Information Technology Services (NYU IT) to Support Investigations. The report will not contain any actual PDC, and will not directly or indirectly identify individuals whose PDC was accessed. The Oversight Committee will meet at least annually to discuss the report and may make recommendations to the Provost as to the processes set forth in this policy and possible amendments to the policy. The Oversight Committee will also make periodic reports to the University Senate on the implementation of this policy.

**Policy Definitions**

“Personal Digital Content” or “PDC” means the following content, and its associated metadata, to the extent stored in files and/or accounts on, or transmitted through, NYU Systems and that are associated with a specific NYU faculty member, student, or staff member:

- (a) digital documents and communications of NYU faculty, students, and staff, such as emails, voice mails, text messages, audio and video files;
- (b) internet search records and internet sites visited for specific NYU faculty, students, or staff;
- (c) manuscripts and other similar works of authorship by NYU faculty, students, or staff that are not publicly available; and
- (d) other scholarly content of NYU faculty, students, and staff that comprises “Traditional Works of Scholarship” under NYU’s Statement of Policy on Intellectual Property, except to the extent such works also qualify as “Instructional Media” under that policy.

“NYU” means Schools and other units of NYU, NYU’s Global Network University sites, and all University Affiliates.
“NYU Systems” means all information technology services, networks, and devices owned, provided, or administered by any unit of NYU. Services include, but are not limited to email services, internet access, file servers, voice message servers, hardware and cloud-based storage devices and/or services, laptop, tablet, desktop, and other computers, phones or other mobile devices, and other outsourced information technology services (e.g., Google NYU Mail or Google Apps for Education).

“School” means each NYU school, college, and institute that functions similarly to a school or college (e.g., IFA, ISAW, Courant, and CUSP), each NYU campus (i.e., New York, Abu Dhabi, and Shanghai), and may include for purposes of this policy other global sites as designated by the Provost.

“University Affiliates” consist of those entities controlled, directly or indirectly, by the University through (a) ownership of more than 50% of the ownership interests in the entity or (b) the power to appoint or elect a majority of the organization’s governing body (e.g., directors or trustees).

**Related NYU Policies**

- Appropriate Use of Email at New York University [https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/appropriate-use-of-e-mail-at-new-york-university.html]
- Electronic Communications and Social Media Policy [in committee]
- Family Educational Rights and Privacy Act (FERPA)
- HIPAA Policies [https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/hipaa-policies.html]
- Missing Student Notification Policy [https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/missing-student-notification-policy.html]
- NYU Code of Ethical Conduct [https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/code-ofethical-conduct.html]
- Policy on Personal Identification Numbers [https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/policy-on-personal-identification-numbers.html]
- Policy on Requests to Information Technology (NYU IT) to Support Investigations [https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/requests-to-it-support-investigation.html]
- Policy on Responsible Use of NYU Computers and Data [https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/responsible-use-of-nyu-computers-and-data-policy-on.html]
- Retention of and Access to Research Data [https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/retention-of-and-access-to-research-data.html]
- Principles and Procedures for Dealing with Allegations of Research Misconduct [https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/researchmisconduct.html]
• Educational and Research Uses of Copyrighted Materials
  [https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/educational-and-research-uses-of-copyrighted-materials-policy-st.html]
• Terms of Use for NYU Google Apps for Education  
  [https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/google-tou.html]
• Faculty Handbook: https://www.nyu.edu/faculty/governance-policies-and-procedures/faculty-handbook.html
• Faculty (Tenured and Tenure-Track ) Grievance Procedures:
• Faculty (Continuing Contract Faculty) Grievance Procedures:  
• Student Grievance Procedures: https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/student-grievance-procedure.html
• Employee Handbook: https://www.nyu.edu/employees/hr-at-your-service/employee-handbook.html