MINUTES OF THE T-FACULTY SENATORS COUNCIL MEETING OF OCTOBER 13, 2016

The New York University Tenured/Tenure Track Faculty Senators Council (T-FSC) met at noon on Thursday, October 13, 2016 in in the Global Center for Academic & Spiritual Life at 238 Thompson Street, 5th Floor Colloquium Room.

In attendance were Senators Adelman, Amkpa, Cappell, Davila, Duncombe, Economides Fenton, Figlewski, Hoffman, Jamieson, Kamer, Lapiner, Livingston, Logan, Longuenesse, Merritt, Mincer, Porfiri, Rajagopal, Ramey, Shapley, Smoke, Tranchina, Uleman, Watson, Weslake, and Zagzag; Alternate Senators Alter (for Weinberg), Gillers (for Jacobs), Tenebein (for Sundarajan), Reiss (for Appiah), Schlick, and Tannenbaum. Former Member Moskowitz attended as a guest.


Upon a motion duly made and seconded, the minutes of the September 15, 2016 meeting were approved unanimously.

CALL FOR NOMINATIONS: CANDIDATES FOR T-FSC CHAIRPERSON, 2017-2018

Chairperson Mincer announced the Executive Committee (EC) appointed Senator Sylvain Cappell as Chair, Senators Arvind Rajagopal, and Jim Jacobs to the Nominating Committee. He asked Council members to send nominations, including self-nominations to Karyn Ridder. The list of candidates for Chairperson, 2017-18 will be announced at the November T-FSC meeting and the election will take place at the December T-FSC meeting. The elections for Vice Chairperson and Secretary will take place in the spring semester.

REPORT FROM THE CHAIRPERSON: ALLEN MINCER

Resolution regarding Long Island University

Chairperson Mincer reported he passed the T-FSC resolution on to Fred Carl, the chair of the Continuing Contract Faculty Senators Council (C-FSC).

Housing Survey

The T-FSC Faculty Housing and Benefits Committee conducted a survey of former and current residents of housing in spring 2015. The committee has begun to meet with the administration to discuss the data collected. The goal is to work together to formulate initiatives that would aid faculty in all stages of their careers, including new faculty, growing families that need to move to larger apartments, faculty considering downsizing, and those who need a solution for housing upon retirement.
UNIVERSITY SENATE COMMITTEE REPORTS

Senate Financial Affairs: Nick Economides

NYU's capital budget

T-FSC representatives on the Senate Financial Affairs Committee brought up concerns regarding bonds that NYU issued in the summer for various building projects and also concerns regarding the prospects of further loans for the 2031 project.

The Financial Affairs Committee was presented with information on NYU's budget including fiscal 2017 budget, historical financial data, Moody’s Rating Report, S&P’s Rating Report, and fiscal 2015 audited financial statements.

T-FSC COMMITTEE REPORTS

Administration & Technology: Chair Carol Reiss

Personal Digital Content (PDC) Policy

See attached Document A: Personal Digital Content Policy

Alternate Senator Reiss presented a summary of the policy. She noted the Dean of the Law School raised issues, namely regarding the manner in which notice would be given when information is accessed, and requesting that the decision to access PDC would not be made by a single individual. Based on these requests, the PDC Policy committee worked with committee member Arthur Miller, who also happens to be an international scholar in the area of privacy rights. The attached revised draft, which Professor Miller assisted in preparing, has also been approved by Dean Trevor Morrison, who raised some of the issues for clarification.

Reiss pointed to page 3, which lists the reasons for access to personal digital content: 1) system protection, maintenance, and management, 2) business continuity, 3) safety matters, 4) legal and regulatory process and litigation, and 5) internal investigations and audits.

The Committee proposed access to PDC of NYU faculty, students, and staff must be authorized by a three-person standing University panel comprised of the VP/CIO or his/her designee, a representative of the Office of General Counsel, and the Provost or his/her designee.

Reiss noted when the issue involves the potential health and safety of some member of the NYU community, emergency measures would be used, including immediately reviewing card-swipes and video.

When NYU intends to access PDC of current NYU faculty, staff, and students, reasonable efforts will be made to give notice to the affected community member(s) at or before the time of access. The policy lists situations where notice is not required.

With respect to access to information, the only content that can be accessed would be on NYU servers, equipment, voicemail, and email. Content on non-NYU servers, equipment, voicemail, and email could only be accessed by court order.

A Senator asked when a NYU community member first receives their NYU account if they give NYU permission to access PDC. Reiss responded NYU does not routinely monitor the PDC of NYU faculty members, students, or staff members, however under the circumstances outlined in the policy and approved by the panel, NYU may obtain access to such PDC.
A Senator commented on the key areas of tension and conflict the last time the Council discussed this document had to do with personal liberties and regulation. He inquired about situations in which faculty are in direct conflict with the university leadership.

Reiss responded in first developing the Social Media Policy, the Committee decided this document on PDC also needed to be developed. She noted there will be an oversight committee that will be appointed, representing all of the Councils in the University Senate, who will review incidences of access and the reasons for access. The Oversight Committee will also make recommendations on modifications of this policy based on the experience of implementing the policy.

A Senator asked if there was discussion on including faculty members on the three-person standing University panel.

Reiss responded with respect to faculty matters, issues of plagiarism, scientific misconduct, etc. would have already gone through a departmental and school-wide investigation with faculty involvement.

A Senator asked if there have been cases in which PDC has been accessed and under what conditions.

Reiss responded it happens frequently with respect to public safety considerations. She noted there have been lawsuits and police actions brought forward with respect to copyright misuse.

A Senator asked about the grievance process. Reiss responded if the issue regards a faculty member it would be handled at the school level.

A Senator asked about a point on Page 4, under the subheading Grievance for Access, which states that NYU does not routinely monitor the personal digital content of a specific NYU faculty member. He asked for clarification on the word “routinely”.

Reiss will discuss with the representatives on the Committee the following items:

- What is the obligation of the accused to provide the key to encrypted computers/files?
- On page 4, in the first sentence of Reasons for Access, a member requested a formal definition of the word “routinely” with respect to monitoring PDC.
- A former member of the T-FSC A&T committee asked for inclusion of a paragraph on Grievance and Disciplinary procedures. Alternatively, if there is a link to standard procedures for this, it should be included.

The next meeting of the Committee takes place after the November Council meeting so the review of the PDC policy will be placed on the December 15 meeting agenda.

Educational Policies & Faculty/Student Relations: Co-Chairs Robert Lapiner & Mark Alter

See attached Document B: Report of the Committee on Educational Policies and Faculty/Student Relations

Protection of Minors

Senator Lapiner reported the Committee met and discussed the Protection of Minors policy, which was approved over the summer. The Committee found the policy to be comprehensive, straightforward, and uncontroversial. The one item the Committee recommended is to provide more details on the required online training for those university members who deal with non-matriculated minors on campus, particularly on the time allowed to complete before programs begin.
Abolish the Box

Lapiner summarized the discussion from the last meeting regarding questions on the admission’s application. Senators expressed concern over the new language used. Senators also considered the university’s legal responsibilities in the event of criminal actions that occur on campus. The Committee reviewed the additional language on the university admission’s website, which expresses the university’s commitment to look holistically at all applications and invites students who were otherwise qualified even if they have checked that box to continue the application process, but they will be subject to other questions.

The Committee found the intent and the language of these statements to be affirmative, and consistent with what the Committee understood as the majority view of the T-FSC as expressed at the last meeting.

The Committee discussed the issue of risk and felt that all the questions being asked about conviction for violence or a sexual offence were important for the university to be able to know in assessing a candidate’s risk to the university.

The Committee does not recommend that the T-FSC express its disapprobation.

A Senator expressed support for the language on the admission’s site, however still objects to the questions on the application. He questioned if the University would obtain useful information from these responses.

A Senator asked for more data on the history of violent incidents on campus and any connection to those that checked the box, both at NYU and other universities.

Senators discussed issues related to diversity, access to NYU education, and using social demographics to exclude people across economic status and other lines despite the basic principle of NYU as a university without walls.

Senators discussed the prison program implemented by the University to educate people in prison. A Senator commented this is a way of rethinking education, not as a commodity, but as something for the social good. A Senator who teaches in the prison education project noted many of her students would be people who would have to check the second box, and the presence of it suggests to her a failure to understand the level of counseling, social work, etc. they have been through to get to a point where they are able to apply to NYU, and the lack of likelihood they would be involved in crime. She also expressed concern regarding those without training in the field interviewing these students.

A Senator expressed concern over the special committee review of these applications, which does not state that the people involved would include faculty or others who have experience working with populations who have been in prison, prison education system, or criminal justice system.

Lapiner responded it would be beneficial to request clarification from the Office of Admissions on how the information will be applied, how they intend to proceed, and whether they will be doing individual interviews with these candidates or other follow-up.

The Committee will reach out to the Admissions Office with these inquiries.

SPECIAL PRESENTATION BY TRACEY GARDNER AND MARY SIGNOR

Bias Response Line

Tracey Gardner, Deputy Chief of Staff in the Office of the President, noted she is also staffing the Equity, Diversity, and Inclusion Task Force. She noted one of the first recommendations of the Task Force is to hire a senior level professional who will have responsibility for coordinating efforts across campus.
She announced an additional date, specifically for faculty, has been added to the Listening Sessions: Monday, October 24 from 1-2:30pm. There is also an email address people can contact to share their thoughts, suggestions, concerns, and also nominate people for the role. After the listening sessions, her Office will use the information and feedback to finalize the job description.

Gardner reported the Bias Response Line (BRL) came out of the November 2015 listening session. When incidences happen in the NYU community, whether it’s in the classroom, residence halls, offices, library, etc. people expressed they did not know where to go or how to communicate these incidences. As a result, it was decided to develop a centralized mechanism. She noted this is a pilot project, and the BRL team is visiting different groups across campus to solicit feedback, concerns, and suggestions. Additionally, at the end of the semester, the BRL team will present at the Task Force’s December meeting to discuss this feedback.

She noted the Bias Response Line is located within the Office of Equal Opportunity. She turned the presentation over to Mary Signor, Executive Director of the Office of Equal Opportunity (OEO) and Title IX Coordinator. Signor stated the Office of Equal Opportunity was created in October 2009. Her role when she joined the university was to help centralize reporting issues of discrimination and harassment across the university.

The line launched in April 2016, then relaunched in September 2016 as the Bias Response Line. The name Bias Response Line came out of researching other universities across the country.

The Bias Response Line was created as a way to report issues of discrimination and also discriminations of bias. The Office of Equal Opportunity has been charged with overseeing this initiative so they can review each of the concerns when they are reported and be able to make the distinction whether it is a bias comment or potentially a hate crime.

The Office of Equal Opportunity has responsibility for monitoring two key policies on campus: the non-discrimination and anti-harassment policy as well as the sexual misconduct, relationship violence, and stalking policy. The Office ensures compliance under the federal, state, and city laws, and is the unit responsible for receiving these reports and concerns. The Office also does workshops across the university on discrimination, cultural sensitivity, and diversity and inclusion.

When created in 2009 to centralize all of these complaints, the Office did an outreach to all schools and identified individuals to serve as contact partners. If an incident is reported that does not require an investigation by OEO it will be referred to the appropriate contact partner.

The Office also worked with IT to develop a tracking system, which is a customized database that will gather information, identity status, and assist in tracking all reports.

Signor noted OEO is not a punitive office but serves as a neutral fact-finder. OEO gathers the information, and if the incident is found to be a violation of anti-discrimination or anti-harassment policy it is referred to the appropriate place: Provost, school, or business unit.

She noted everyone can utilize the BRL: faculty, staff, administrators, students, vendors. There are three ways to report: phone at 212-998-2277, email at bias.response@nyu.edu, and the online form at nyu.edu/biasresponse

Since the soft launch in April 2016, 26 concerns have been reported, 15 since September 2016. Of the 26 concerns, 20 were from students, 4 from faculty members, and 2 from graduate alumni.

She noted the BRL it is not emergency line and is not staffed 24 hours a day, however there is a live person on the line from 9am to 8pm and emails will be responded to within the next 24 business hours.
A Senator asked about the data tracking system. Signor clarified information on all complaints does stay in the system, in the OEO, but if an incident is not found to be in violation of a policy, it is not incorporated into one’s personnel file.

A Senator asked about instances related to sexual harassment or sexual assault. Signor responded her Office does handle these issues. She noted a student does have the right to remain anonymous if they come forward in a sexual harassment or sexual assault case. She does an assessment and consultation with wellness and public safety and student affairs to determine whether the person poses a threat to others on campus. If it is determined that the person could pose a risk to others on campus, the Office would move forward with the investigation.

Signor encouraged Senators to also communicate any best practices from their schools. She offered the example of the School of Law, which has a diversity working group that developed a three-page document about creating an inclusive classroom.

**ADJOURNMENT**

The meeting adjourned at 2:00 PM.
From: Joint NYU Senate Councils’ Policy Committee  
AMC: Norma Kenigsberg (and ITS)  
C-FSC: Janie Skye Bianco, Jung (Ted) Kim, Vicky Steeves, Antonius Oktaviano Wiradja (NYUAD)  
T-FSC: Kwame Anthony Appiah, Carol Shoshkes Reiss (chair), Arun Sundararajan (co-chair), Amanda Watson, Brad Westlake (NYUSH), Thomas Wisniewski  
Deans: Carol Mandel  
Public Safety: Rebecca Holland  
ITS: Kitty Bridges  
Student Affairs Office: Craig Jolley  
General Council’s Office: Mark Righter

To: Elected Members of AMC, C-FSC, T-FSC, and Deans’ Council

Date: 10/6/16

You may recall discussion and consideration over the past few years regarding the Personal Digital Content Policy (“PDC Policy”). The PDC policy is intended to: a) further buttress NYU’s existing strong protections in this area, and b) to ensure that NYU's policies and practices are consistent with national best practices.

You may further recall that the AMC, C-FSC and T-FSC approved the PDC Policy in 2015. It then went for consideration and approval by the Deans and Provosts Group. That group raised several issues where it requested additional clarifications, namely regarding the manner in which notice would be given when information is accessed, and requesting that the decision to access PDC would not be made by a single individual. Based on these requests, our PDC Policy committee worked with committee member Arthur Miller, who also happens to be an international scholar in the area of privacy rights. The attached revised draft, which Professor Miller assisted in preparing, has also been approved by Dean Trevor Morrison, who raised some of the issues for clarification.

Accordingly, the amended policy must now be approved by the AMC, C-FSC, T-FSC, and Deans’ council. We have attached the PDC for your consideration.
New York University
UNIVERSITY POLICIES

Title: University Access to Personal Digital Content
Effective Date: October 3, 2016
Supersedes: New Policy
Date of Latest Revision: N/A
Issuing Authority: Executive Vice President, Finance and Information Technology
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 Network University sites, 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 routinely monitor the PDC of a specific NYU faculty member, student, or staff member. 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.

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 Healthcare 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 portal campus (e.g., New York and Abu Dhabi), 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)
- [Data Classification at NYU](https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/data-classification.html)
- Electronic Communications and Social Media Policy
- 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-of-ethical-conduct.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-its-support-investigation.html)
- [Policy on 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)

• Terms of Use for NYU Google Apps for Education. [https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/google-tou.html]

Report of the September 26 Meeting of the
Committee on Educational Policies and Faculty/Student Relations

The Committee on Educational Policy and Faculty/Student Relations met on September 26, and undertook the review of two sets of documents: the recently issued policy on “Protection of Minors” and the guidelines for dealing with applicants for undergraduate admissions who have self-identified on the Common Application as having had a prior criminal record.

1) We found the Policy on Minors comprehensive and generally unobjectionable. It is attentive both to the range of programs that bring non-matriculated minors to the University for responsible academic and other educationally-related purposes as well as to the legal and ethical obligations to assure that all those who work with, teach, accompany, or interact with minors in the NYU environment are appropriately trained and vetted. In short, the policy seeks to protect minors on the one hand, and to limit the risk to the university arising from inappropriate conduct committed by those in its employ.

Our committee had only one modest question about implementation as it relates to the promise in the policy to provide online training for university employees and matriculated students who are programmatically involved with the minors—and specifically, to require that all those in that role complete the training before they shall be entrusted to work with minors under NYU auspices. We respectfully request clarification about the training, to make sure that it can be accessed and completed in a timely fashion—since support staff and student workers are often hired very close in time to the start of programs, and training requirements will have to be able to anticipate the vagaries of truncated lead-times.

2) During our last Council meeting, Alan Mincer shared a document that had been brought to the attention of the Senate Executive Committee—a document that elicited nearly universal consternation among Council members. It involved an interrogatory University admissions had prepared for dealing with the sensitive issue of how NYU would reconcile three goals: 1) how to mitigate the dissuasive effect of the Common Application’s asking those seeking admission to disclose prior criminal records, 2) how to act upon a widely shared impulse to extend an opportunity for admission to candidates who can credibly demonstrate they are not a danger to the university, despite very serious misconduct in their youth—and who otherwise meet admission criteria; and 3)
how, as an institution, NYU can follow the latter impulse while evaluating all available evidence consistent with the obligation to assure as safe and violence-free an environment for all students, faculty, staff—and visitors—as possible.

Initially our Committee members found the interrogatory problematic and intrusive—indeed more problematic than the box on the Common Application. Moreover, we had trouble figuring out how it fit with the University administration’s purported agreement to look as generously and without prejudice/implicit bias at all applicants who “checked the box.” Yet we were also mindful of the University’s legal exposure if recidivist behavior led to violence or felonious behavior on campus resulting in bodily harm to anyone or major loss or damage to property. As had been pointed out at our last Council meeting, NYU could be found liable and derelict in its responsibilities if incidents occurred, and there were no process in place to scrutinize documentation readily available in the application process.

This said, while the Committee members had all been taken aback by the language of the text that had been read during our Council meeting, our perspective changed after we consulted the official language in the Admissions landing pages on the NYU website—the spirit of which was more closely aligned with the goal of alerting prospective applicants that their candidacy would be given full and reasonable consideration.

The text on the web page follows. (Here is the hyperlink within the Admissions section of the NYU Website: [http://www.nyu.edu/admissions/undergraduate-admissions/how-to-apply/prior-criminal-conviction.html](http://www.nyu.edu/admissions/undergraduate-admissions/how-to-apply/prior-criminal-conviction.html)

[Start text:]

*NYU is one of roughly 600 colleges and universities that uses the Common Application, which asks students if they have been convicted of a crime or committed school disciplinary infractions.*

*At NYU, we believe in second chances, and we are sensitive to the deep concerns many people have about the fairness of our justice system and whether it equitably serves all members of our society. We want to balance these issues with our duty to ensure a safe environment for our community.*

*As a result, we have developed a review process that we believe strikes a balance between giving people a second chance through higher education and keeping our campus safe. We review all candidates for admission holistically and never automatically deny*
admission to those with a criminal conviction. Academic qualifications are the primary consideration of our holistic evaluation process, which also includes an analysis of one’s extracurricular accomplishments, work experience, letters of recommendation, essays, personal characteristics, talents, and life experiences.

**Our Admission Process**

NYU is committed to treating applicants with a criminal or disciplinary history fairly and with dignity and respect. In keeping with this outlook, NYU is making certain changes beginning with the 2016-17 admissions cycle (for admission in fall 2017):

- **Ignoring the questions on the universal section of the Common App**: NYU will ignore any answers applicants provide to the questions in the main section of the Common Application regarding criminal and disciplinary history because we believe them to be too broad. Instead, we ask two more-focused questions that we think are more relevant to the issues of campus safety.

- **“Box Blind” first reading**: All applications for traditional undergraduate admission are initially reviewed by admission officers without knowledge of whether they have “checked the box” in the NYU section of the application indicating a criminal or disciplinary history that involves violence or physical harm.

- **Special Committee Review**: Once an initial evaluation is completed, and if a positive recommendation by an admission officer based on our holistic review is proposed, the applications of those who indicate a criminal history in their applications are reviewed by a special review committee. This special review committee includes admission officers, university staff, and faculty trained to perform an assessment based on a multi-factor analysis to fairly determine whether a past criminal offense justifies denial of admission. This special review committee is responsible for making a final determination about admission. Candidates are then notified of their admission decision.

As we indicated previously, answering “yes” to NYU’s questions is not an automatic bar to admission. NYU reviews candidates holistically and will seek to understand the context of any “yes” answers. So, we strongly urge applicants to complete their applications regardless of whether they answered "yes." [End Text]
Resisting editorial reflexes to refashion some of the above language for greater felicity (☺), we found the intent and the language of these statements to be affirmative, and consistent with what we understood as the views of the majority of the T-FSC as expressed at our last meeting.

It then became clear that the interrogatory we saw had been read out of context, for it was conceived to provide the framework of the follow-up due diligence questions the Admissions office would be asking. Does asking them run counter to the commitment to a full and balanced evaluation of each applicant—the holistic evaluation process promised on the webpage?

The Committee members concluded unanimously that while the questions are pointed, the information they are designed to elicit must be considered in the Admissions process. The balance between the welcoming language of the webpage and the straightforward request for answers about serious issues may be in awkward tension with each other. But having examined the context and having had a robust discussion about risk scenarios, we all concurred that the nearly universal hostility to the interrogatory that we had also shared at the outset was not warranted. We thus do not recommend that the T-FSC express its disapprobation.