Protection of Minors: The New Youth Programs Compliance Office and Policy

New York University (‘NYU’ or ‘University’) welcomes thousands of students who are minors – under the age of eighteen (18) - to its New York City campuses every year. As part of the University’s educational mission, many NYU schools and programs sponsor various types of programs or activities for grade school or high school students who are below the age of 18 and are not enrolled in or accepted for enrollment in a degree granting program at NYU. These programs and activities include everything from tutoring in City schools to mentoring STEM students to summer programs for burgeoning filmmakers to hosting educational programs conducted by outside organizations.

Minors at NYU participate in diverse programs and opportunities, including internships, academic year courses, summer pre-college programs, and lessons through our athletic centers, and music and theater programs. As an academic institution “in and of the city,” it is crucial to our mission that NYU not only provide opportunities for minors but also support and protect minors while they are participating in activities or programs sponsored by the University or utilizing University facilities and resources.

Consequently, NYU has established the Office of Youth Programs Compliance and the Protection of Minors Policy (“Policy”), which can be found here. The Policy applies across units that sponsor programs and activities involving minors.

Marco Di Fava serves as the Director of the Office of Youth Programs Compliance in Human Resources. Marco has been actively collaborating with schools and department liaisons in the implementation and overall management of the University’s commitment to protecting minors on campus.

The purpose of the Policy is to establish guidelines and procedures for members of the University community who host and interact with minors on campus. The policy applies to all NYU employees, including faculty and visiting faculty, professional staff, and administrators, students, consultants, contractors, and third-party vendors participating in these programs.

Schools, departments, or units that want to offer programs involving or housing minors who are not enrolled in or accepted for enrollment in a degree-granting program at NYU, or that host a non-NYU program involving minors in University facilities, will need to register the program with the Office of Youth Programs Compliance.

You can find more information about the Policy, program registration system, and additional resources at nyu.edu/protectionofminors.

For questions or if you are registering a program for the first time, contact PeopleLink at askpeoplelink@nyu.edu or 212-992-LINK (5465).
The following is an excerpt from Educause article printed with permission from the author, Gary Miller, Compliance Director, College of New Jersey

When employees hear the terms “compliance,” “privacy,” and “security,” it is often difficult for many to fully understand how these terms and the aims of these business initiatives diverge. So, how do they differ?

Compliance
As defined by Robert Roach, vice president and chief global compliance officer at New York University, “Compliance is a systematic approach to governance designed to ensure that an institution meets its obligations under applicable laws, regulations, best practices and standards, contractual obligations, and institutional policies.” In other words, “compliance seeks to achieve accountability and transparency in all institutional operations.”

In this vein, compliance is often viewed simply as “complying with the law,” and although this is perhaps true in many respects, compliance professionals would argue that compliance programs should seek to go a step further. Compliance professionals, especially those with an added ethics responsibility, often seek to communicate compliance as a “commitment to doing the right thing.” Getting employees to understand that being committed to doing the right thing will ultimately result in complying with the law is arguably the primary goal of a compliance function.

The generally accepted elements of an effective compliance function are seen as the tools that a compliance professional can use to accomplish this mission. Examples include the development of policies and procedures so that individuals have the information they need to make the right decisions, as well as training and education so that employees understand the policies and procedures and how to apply to their daily responsibilities. As we know, in a highly regulated sector such as higher education, there is a myriad of laws, regulations, and agency guidance with which institutions must comply. But, as compliance professionals often state, compliance with these requirements is a business function and not the responsibility of the compliance office. The compliance office supports operational compliance by acting as portfolio manager of the regulatory matrix, leveraging the compliance program to ensure that all of the institution’s obligations are met by the subject-matter experts at the operational level.

Privacy
As stated by Louis Brandeis and Samuel Warren, privacy is often defined as the right to be left alone, or freedom from interference or intrusion. However, in today’s digital environment the word has evolved to include a number of concepts including data privacy, in addition to the individual privacy alluded to by Brandeis and Warren.

Data privacy is generally focused on the use and governance of personal data and personally identifiable information. It might include putting policies in place to ensure that personal information is being collected, shared, and used in appropriate ways. For instance, there are legal and regulatory requirements (e.g., the Family Educational Rights and Privacy Act [FERPA] and the Health Information Portability and Accountability Act [HIPAA]) that colleges and universities must comply with throughout their daily operations. Here, privacy looks familiar to other compliance topics, similar to meeting obligations for campus safety reporting (e.g., the Clery Act), research (e.g., human-subject safety, conflict of interest), and other requirements.

However, the role of privacy offices in higher education may extend beyond merely complying with regulations at the institutional level (although this is also an important responsibility). The privacy officer is often also seen as an advocate for privacy at the individual level as the representative for the College’s constituents, including students, faculty, and staff. Data collection and use, monitoring, and physical surveillance may all be controls that help the institution comply with certain regulations, but these activities potentially implicate the ever-increasing considerations of privacy.

This is another area where privacy is distinct from compliance but necessarily overlaps with compliance initiatives. The privacy officer seeks to promote forward-thinking privacy considerations in college or university operations by considering the concepts included in various privacy frameworks, such as the Fair Information Privacy Principles, in particular the ideas of notice,
Coming This June- The Third Annual Compliance and Risk Symposium

The **Office of Compliance and Risk Management** and the **Office of Insurance and Enterprise Risk Management** are pleased to announce the upcoming Third Annual Compliance and Risk Management Symposium. The event will be held on June 22nd from 11:00 am through 3:00 pm at the NYU Law School.

This year’s program will cover significant topics in the realm of business ethics, entrepreneurial innovations, and privacy and cybersecurity. The first panel focuses on faculty and student innovation and entrepreneurial engagement at NYU. Our guest speakers include faculty members from Tandon School of Engineering, the Office of Industrial Liaison, Leslie eLab, and Office of General Counsel.

Our second panel focuses on business sustainability and designing ethical systems and how to incorporate this framework in a university setting. The panel consist of Stern faculty who are leaders in the field of Business Ethics and Sustainable Business.

Our third panel will cover the increasingly complex web of data privacy and cybersecurity and will also cover the non-technological aspects of cybersecurity, and how trust plays a role. Guest speakers include NYU IT’s Chief Information Security Officer and NYU’s Center for Data Science.

If you are interested in attending, please reach out to the Office of Compliance and Risk Management at 212-998-2265 or email us at **NYUCompliance@nyu.edu**.

It promises to be an exciting event!

Compliance, Privacy, and Security...What’s the Difference? *continued from page 2*

Transparency, and choice. These privacy concepts are also implicated in the operations of the college, where compliance may not have as big a role due to a current lack of regulation in a particular area. For example, the increased use of student learning analytics is not yet a regulated activity, but certainly there are privacy considerations in using these data for various purposes, including assessing higher education programs and activities, student engagement, and academic program achievement.

**Security**

Security is important for both compliance and privacy. Security, as the primary responsibility of the Information Security Officer, is generally understood to focus on protecting data from impermissible access, including intentional malicious attacks. Certain regulations, such as HIPAA and the Gramm-Leach-Bliley Act (GLBA), require that security protocols exist. Compliance with these regulations requires an institution to put specified security controls in place.

For privacy, security is a well-known important principle. Institutions maintain the privacy of their constituents’ data by having security protocols in place to prevent against external threats and data breaches. Institutions also maintain simpler controls, such as ensuring that internal data use is appropriate. Physical security is also important for privacy, including surveillance and access control to data centers and/or hard-copy record rooms. But it is important to recognize that security is not the same as privacy. In other words, security is necessary for protecting data, but not always sufficient for addressing privacy.

As a brief example, consider surveillance systems. Surveillance videos may provide a sense of security to individuals on campus. But what about potential privacy concerns implicated by this particular security activity? An institution may have state-of-the-art electronic security software and protocols to protect any electronic data recorded. However, a privacy officer may ask what data are being collected? Where are individuals being surveilled? Where are cameras located? Why is surveillance necessary, and how are any data collected being used? Institutions must consider basic privacy principles, such as notice of data collection and consent to data collection, before collecting and using data.

*Notes from this article can be found on page 4.*
Policy Post– Highlighting New and Revised University Policies

A goal of the Office of Compliance and Risk Management (OCRM) is to inform the NYU community about new and revised University-wide policies and guidelines. These policies can be located on the University Policy website at nyu.edu/policies. In this issue, we highlight new and updated Human Resources policies:

Protection of Minors Policy
The purpose of this Policy is to establish guidelines and procedures for members of the University Community who take part in NYU Covered Programs and for members of Non-University organizations who take part in Non-NYU Covered Programs, with the goal of promoting the safety and well-being of Minors. In the Policy, you will find guidance on:
- Employees bringing children and children to work;
- Students bringing children to class;
- Visitors bringing children on campus;
- Employment of minors and children; and
- Offering extracurricular learning opportunities for minors.

Parental Bonding Leave Policy
- Months of service to be eligible is now 12 (reduced from 24)
- There is now no distinction between "primary" and "non primary" caregiver
- Application is due 30 days prior to "event" as opposed to much earlier
- Vacation days may now be used immediately following Bonding Leave

Sick Leave Policy
Sick time can now be used for "preventative medical care or for medical diagnosis, care, or treatment of a mental or physical illness, injury or health condition" (i.e. you can use sick time for doctor’s visits.)

Family Medical and Leave Act (FMLA)
There is now a detailed explanation from NYU on how to use your FMLA leave. Click here for more information on New York City and District of Columbia federal policy and procedures.

Have Policy questions? OCRM can assist you with policy development, add your policy to the University Policy database. Email us at NYUCompliance@nyu.edu.

Notes from Compliance, Privacy, and Security, page 2

2. Ibid.
4. See About the IAPP, “Privacy v. security...isn’t it the same thing?”
5. Ibid.

Compliance Matters provides updates about important compliance issues covering new regulations, new and updated University Policies, and risk management.

We welcome feedback and suggestions from the NYU Community for articles in future issues. Please send your ideas or submissions to Diane Delaney, Associate Compliance Officer, at diane.delaney@nyu.edu or Deputy Compliance Officer Rachna Vaid at Rachna.vaid@nyu.edu.