THE CITY UNIVERSITY OF NEW YORK

3. Faculty includes full-time, part-time, and adjunct faculty.

4. FOIL

5. Non-Public University Information
Policies and Procedures found at security.cuny.edu, namely: personally identifiable

non-driver identification card number; account number, credit or debit card number, in combination with any required security code, access code, or password that would permit

student education records that is protected under the Family Educational Rights and Privacy Act of 1974 (FERPA) and the related regulations set forth in 34 CFR Part 99;

New York State Law with respect to the confidentiality of library records

c.

7. Integrity of Computer Resources. Users may not install, use or develop programs intended to infiltrate or damage a CUNY Computer Resource, or which could reasonably be expected to cause, directly or indirectly, excessive strain or theft of confidential data on any computing facility. This includes, but is not limited to, programs known as computer viruses, Trojan horses, and worms. Users should consult with the IT director at their college before installing any programs on CUNY Computer Resources that they are not sure are safe or may cause excess strain.

8. Disruptive Activities.

a. CUNY Computer Resources must not be used in a manner that could reasonably be expected to cause or does cause, directly or indirectly, unwarranted or unsolicited interference with the activity of other users, including:

i. chain letters, virus hoaxes or other e-mail transmissions that potentially disrupt normal e-mail service;

10. Security.

a. CUNY employs various measures to protect the security of its computer resources and of U
are responsible for engaging in safe computing practices such as guarding and not sharing their passwords, changing passwords regularly, logging out of systems at the end of use, and protecting Non-Public University Information, as well as for
T Security Policies and Procedures.

b. Users must report incidents of non-compliance with IT Security Policies and Procedures or other security incidents to the University Chief Information Officer and Chief Information Security Officer, and the Chief Information Officer at the affected U

11. Filtering. CUNY reserves the right to install spam, anti-malware, and spyware filters

Technology or a college IT director to protect the security and integrity of CUNY Computer Resources. CUNY will not install filters that restrict access to e-mail, instant messaging, chat rooms or websites based solely on content, unless such content is illegal, such as child pornography sites.

12. Confidential Research Information. Principal investigators and others who use CUNY Computer Resources to collect, examine, analyze, transmit or store research information that is required by law or regulation to be held confidential or for which a promise of confidentiality has been given are responsible for taking steps to protect such c

b. General Monitoring Practices. CUNY does not routinely monitor, inspect, or disclose individual usage of CUNY Computer Resources without the U consent. In most instances, if the University needs information located in a CUNY Computer Resource, it will simply request it from the author or custodian. However, CUNY IT professionals and staff do regularly monitor general usage patterns as part of normal system operations and maintenance and might, in connection with these duties, observe the contents of web sites, e-mail or other electronic communications. Except as provided in this policy or by law, these individuals are not permitted to seek out contents or transactional information, or disclose or otherwise use what they have observed.

personnel or agents, or law enforcement or other agencies. The results may be used in college disciplinary proceedings, discovery proceedings in legal actions, or otherwise as is necessary to protect the interests of the University.

B. In addition, users should be aware that CUNY may be required to disclose to the public under FOIL communications made by means of CUNY Computer Resources whether in conjunction with University business or as incidental personal use.

C. Any disclosures of activity of accounts of individual Users to persons or entities outside of CUNY, whether discretionary or required by law, shall be approved by the General Counsel and shall be conducted in accordance with any applicable law. Except where specifically forbidden by law, CUNY employ y the GeneUNc05 515.95 Tm

iv. the length of time for which the waiver is being requested; and

v. if a student, how and by whom the student will be supervised.

c.

deliveries, or service interruptions, whether or not resulting from circumstances under the CUNY s control.

b. Users receive and use information obtained through CUNY Computer Resources