THE CITY UNIVERSITY OF NEW YORK
POLICY ON ACCEPTABLE USE OF DIGITAL ASSETS AND RESOURCES

I. INTRODUCTION

The City University of New York's ("CUNY" or the "University") Digital Assets and Resources, as defined below in section VI, are dedicated to the achievement of the University's mission of education, research, and public service. This policy, which guides the University's use of its digital assets and resources, is intended to maintain the continuity of CUNY's IT and business operations, and protect the University, and its students, faculty, and staff.

II. SCOPE

This University-wide Policy ("Policy") applies to all Users of CUNY Digital Assets and Resources. This Policy supersedes the CUNY Policy on Acceptable Use of Computer Resources, which the Board of Trustees approved on January 29, 2007, and last amended on June 29, 2015, and any College policies that are inconsistent with this Policy.

III. RULES FOR USE OF CUNY DIGITAL ASSETS AND RESOURCES

1. Legitimate Use.
    a. Use of CUNY Digital Assets and Resources is limited to Users' authorized activities in connection with their roles and responsibilities in relation to CUNY at any location, whether on or off CUNY property.
    b. Users are permitted limited and reasonable personal use of CUNY Digital Assets and Resources so long as such use does not interfere with CUNY operations, compromise CUNY Digital Assets and Resources, affect the User's employment or other obligations to CUNY, and is otherwise in compliance with this policy.
    c. Users should be aware that personal messages, data, and other information sent or received through a User's CUNY account or otherwise residing in a CUNY Digital Assets or Resources are subject to CUNY review and may also be subject to public disclosure pursuant to the New York State Freedom of Information Law ("FOIL").
2. Cybersecurity and Protecting the Security of Digital Assets and Resources**.** CUNY employs various measures to protect the security of its Digital Assets and Resources and User accounts. However, CUNY cannot fully guarantee such security, as effective cybersecurity requires the participation of everyone. When accessing University digital assets and resources, Users are responsible for engaging in safe computing practices that include the following:
    a. Taking all reasonable actions to keep software up to date, including by engaging with University or College staff when necessary. Avoiding phishing scams and fraud. Always verifying unsolicited inquiries and offers and being careful not to click on links from unknown sources;
    b. Practicing good password management by choosing strong and unique passwords for every account or application. Accounts and passwords may not be shared except as permitted by this policy;

c. Using enhanced authentication features such as multi-factor authentication where available.

d. Locking the computer screen electronically when the User leaves a computer unattended, and logging out of applications and systems at the end of each workday;

e. Backing up important data. It may be the only way to recover data lost in a security incident;

f. Maintaining up-to-date security software that includes anti-malware protection, including by engaging with University or College staff when necessary.

User responsibilities also include:

a. Protecting Non-Public University Information from inappropriate disclosure and access;

b. Following CUNY's IT Security Policies and Procedures;

c. Completing technology training, including, but not limited to, cybersecurity awareness, as directed by the University;

d. Using CUNY provided accounts to issue and receive CUNY-related communications and to perform work on behalf of CUNY. Use of personal accounts may subject those accounts to FOIL;

e. Reporting IT Security concerns or incidents to the Chief Information Officer ("CIO") at the affected User's College or in the case of the Central Office, as determined by CUNY's CIO.

3. Authorization to Use Digital Assets and Resources**.**

a. Users may not access a CUNY Digital Asset or Resource without appropriate authorization or use it for purposes beyond the scope of such authorization. This includes attempting to circumvent CUNY Digital Assets and Resources system protection facilities by hacking, cracking, or similar activities, accessing or using another User's account, and allowing another person to access or use the User's account.

b. Users may temporarily authorize another CUNY employee to access information on the User's account when the User is on leave or is otherwise unable to access the account on the User's own behalf. Such delegated access must be in effect only for the minimum duration and extent of access required to facilitate continuity of operation and does not absolve the User from responsibility for their account activity.

c. CUNY Digital Assets and Resources may not be used to gain unauthorized access to another computer system within or outside of CUNY. Users are responsible for all actions performed from their computer account that they permitted or failed to prevent by following reasonable security precautions and/or security advisories issued by CUNY. CUNY advisories and resources are available at security.cuny.edu.

4. Compliance with Law**.** CUNY Digital Assets and Resources may not be used for any purpose or in any manner that violates CUNY rules or policies, or federal, state, or local law. Users who engage in electronic communications with persons in other localities,

states, or countries or on other systems or networks may also be subject to the laws of those other localities, states and countries, and the rules and policies of those other systems and networks. Users are responsible for ascertaining, understanding, and complying with the laws, rules, policies, contracts, and licenses applicable to the use of CUNY Digital Assets and Resources.

5. False Identity and Harassment**.** Users may not employ a false identity, mask the identity of an account or computer, or use CUNY Digital Assets and Resources to engage in abuse of others, such as sending harassing, obscene, threatening, abusive, deceptive, defamatory, or anonymous messages within or outside CUNY.
6. Protecting Confidentiality and Privacy.
    a. The University is committed to the creation and free exchange of information, knowledge, and ideas among members of CUNY and other academic communities. As a public university and protector of public resources against misuse, CUNY also has a responsibility to fulfill that commitment in responsible and secure ways. To uphold this responsibility, the University abides by the parameters outlined in this Policy and others that inform and govern the use of Digital Assets and Resources. This Policy permits CUNY to undertake certain monitoring of its Digital Assets and Resources, as described in Article IV below. Consequently, Users should have no expectation that use of CUNY Digital Assets and Resources will be private, except for any privilege or confidentiality recognized by law, including the confidentiality of library records cited in section V (4).
    b. Users may not invade the privacy of others by, among other things, viewing, copying, distributing, publishing, modifying, or destroying data or programs belonging to or containing personal or confidential information about others, without explicit permission to do so from the subject of such information.
    c. Users must follow all CUNY IT Security Policies and Procedures to protect the confidentiality of non-public information encountered in the performance of their duties or otherwise.
7. Protecting the Integrity of Digital Assets and Resources Against Unacceptable Use and Disruptive Activities. CUNY Digital Assets and Resources must not be used in a manner that could reasonably be expected to result in undue stress or harm or to interfere, directly or indirectly, with other Users of CUNY Digital Assets and Resources, including, but not limited to:

    a. Use of scripted or programmed actions that attempt to repetitively register for a course or that repetitively determine whether grades have been posted or changed.

    b. Use of malware, ransomware, and similar malicious code.

    c. Theft of confidential data.

    d. Streaming or downloading large videos, films, or similar media files for personal use.

    e. Chain letters, hoaxes or other online communications that potentially disrupt normal

service.

f. Sending unsolicited communication that is not related to CUNY business without a reasonable expectation that the recipient would welcome receiving it.

g. The inclusion of individuals on mailing lists or the equivalent who have not requested membership on the lists, other than the inclusion of members of the CUNY community on lists related to CUNY business.

h. Accessing disruptive and/or not-suitable-for-work content. Examples of such content include, but are not limited to: pornography; gambling; personal commercial enterprise; not-for-profit non-CUNY business purposes; personal advertising of products or services; any activity meant solely to foster personal gain; or partisan political activity. The foregoing is prohibited except in the course of official business or legitimate academic or research purposes or in support of faculty or University-endorsed purposes. When accessing such otherwise prohibited content, appropriate care must be taken to avoid offending or disrupting other Users.

8. Confidential Research Information.

a. Principal investigators and others who use CUNY Digital Assets and Resources to collect, receive, examine, analyze, transmit and/or store research information that is required by law or regulation to be held confidential or for which an agreement of confidentiality has been given are responsible to take steps to protect such confidential research information from unauthorized access or modification. In general, this means storing the information in a cloud solution or on a computer or auxiliary hard drive with strong access controls (passwords) and encrypting files, documents, and messages for protection against inadvertent or unauthorized disclosure while in storage or in transit over data networks. However, additional protections may be required by law or an associated agreement.

b. Robust encryption and passwords must be used to protect Non-Public University Information, and is strongly recommended for information stored electronically on all desktop and laptop computers, mobile devices that allow or are capable of storing and transmitting information (e.g., cell phones, tablets), computer systems, in a cloud solution, servers, software, network facilities, databases, memory, memory sticks, portable hard drives and associated peripherals and software that are vulnerable to theft or loss, as well as for information transmitted over public networks.

c. Software and protocols used should be reviewed and approved by the campus CIO in consultation with the Chief Information Security Officer and CUNY's Office of Computing and Information Services ("CIS"). In addition, the steps taken to protect such confidential research information should be included in submissions to the CUNY Human Research Protection Program ("HRPP") reviewing the research protocol.

9. Licenses and Intellectual Property.

a. Users may use only legally obtained data, software, or cloud solutions. Users must also comply with applicable licenses or other contracts, as well as copyright, trademark, and other intellectual property laws. Prior to acquisition, all software must be approved by

the campus CIO or their designee.

b. Much of what appears on the Internet and/or is distributed via electronic communication is protected by copyright law, regardless of whether the copyright is expressly noted. Users should generally assume that material is copyrighted unless they know otherwise, and not copy, download, or distribute copyrighted material without permission unless the use does not exceed fair use as defined by the federal Copyright Act of 1976, as amended. Protected material may include, among other things, text, photographs, audio, video, graphic illustrations, and computer software. Additional information regarding copyright materials and file sharing is available on the CUNY Office of the Senior Vice Chancellor for Legal Affairs and General Counsel ("OGC") website.

10. CUNY Names, Trademarks and Brand.

a. CUNY names, trademarks, brand, and logos belong to the University and are protected by law. Users of CUNY Digital Assets and Resources may not state or imply that they speak on behalf of CUNY or use a CUNY name, trademark, brand, or logo without first receiving permission to do so from the appropriate CUNY authority. Affiliation with CUNY does not, by itself, imply authorization to speak on behalf of CUNY.

b. CUNY employees and students may indicate their CUNY affiliation on email, other correspondence, and in academic or professionally-related research, publications, or professional appearances, so long as they do not state or imply that they are speaking on behalf of the University.

IV. CUNY'S RIGHTS AND RESPONSIBILITIES

1. Filtering**.** CUNY reserves the right to install spam, anti-malware, spyware filters, and similar devices, if necessary, in the judgment of CIS or a College CIO to protect the security and integrity of CUNY Digital Assets and Resources. CUNY will not install filters that restrict access to email, instant messaging, chat rooms or websites based solely on content, unless such content is illegal, such as child pornography.

2. Review of the Use and Access to CUNY's Digital Assets and Resources. CUNY has a unique responsibility to facilitate the creation and exchange of information, knowledge, and ideas while also preserving and safeguarding CUNY Digital Assets and Resources from potential security issues and/or misuse. CUNY will follow the practices below when accessing Digital Assets and Resources, except in exigent circumstances where it is not feasible to delay such access.

a. Preservation. To preserve University information, evidence, and/or resources, CUNY may obtain and/or copy any information associated with, or residing on, a CUNY Digital Asset and Resource, without inspection of the contents and without notice to the User.

i. Users have an obligation to preserve Electronically Stored Information ("ESI") if requested to do so by CUNY.

b. Routine Audits and Monitoring. Respecting the privacy of Users and serving as responsible stewards of University Digital Assets and Resources are both priorities for CUNY. However, as part of routine system operations and maintenance, CUNY

regularly audits and monitors general usage patterns. In connection with these activities, the contents of websites, email and other digital content may be viewed. CUNY will not, however, monitor, inspect, or disclose an individual's usage of CUNY Digital Assets and Resources, except as provided for in this or other CUNY policy, or by law.

c. Inspection without Notice

i. Categories. CUNY may inspect without notice the activity and accounts of individual Users, including, but not limited to, individual login sessions, email, and other communications. Such inspections without notice will be conducted in the following circumstances:

A. when the User has voluntarily made them accessible to the public;

B. when it is necessary to do so to protect the integrity, security, and/or functionality of CUNY or its Digital Assets and Resources, as determined by the College CIO and/or CUNY's CIO;

C. when it is necessary to diagnose and resolve technical problems involving system hardware, software, or communications, as determined by the College CIO, after consultation with CUNY's CIO, or in the case of the Central Office, as determined by CUNY's CIO;

D. when it is necessary to determine whether CUNY may be vulnerable to liability, and/or when failure to act might result in: harm to an individual, property loss, and/or damage, financial loss, impact to business continuity, and/or loss of evidence, as determined by OGC, once notified in writing by the College President, or the Chancellor. If any of the matters mentioned in this sub-section concern a current CUNY faculty member's account or activity, CUNY will consult and notify the Chair of the University Faculty Senate (or Vice Chair if the Chair is unavailable) in a timely manner regarding said inspection without notice before said monitoring has occurred (unless extraordinary circumstances warrant otherwise);

E. when there is a reasonable basis to believe that CUNY policy and/or federal, state, and/or local law has been or is being violated, as determined by OGC, once notified in writing by the College President, or the Chancellor. If any of the matters mentioned in this sub-section concern a current CUNY faculty member's account or activity, CUNY will consult and notify the Chair of the University Faculty Senate (or Vice Chair if the Chair is unavailable) in a timely manner regarding said inspection without notice before said monitoring has occurred (unless extraordinary circumstances warrant otherwise);

F. when an account appears to be engaged in unusual or unusually excessive activity, as determined by the College President, or the Chancellor, after approval by OGC. If any of the matters mentioned in this sub-section concern a current CUNY faculty member's account or activity, CUNY will consult and notify the Chair of the University Faculty Senate (or Vice Chair if the Chair is unavailable) in a timely manner regarding said inspection without notice before said monitoring has occurred (unless extraordinary circumstances warrant

otherwise);

G. where the activity and/or account content of individual Users are required to be produced pursuant to a subpoena and if a law enforcement agency issuing the subpoena has requested in writing that the subpoena not be disclosed to the User or any third party. Such production will not be made without approval by OGC;

H. as otherwise required by law.

ii. Procedure when a CIO or College President is the Subject of Monitoring

A. If monitoring without notice is contingent on a determination by the College CIO or their designee, and the CIO is the subject of the monitoring, the College shall seek a determination from CUNY's CIO. In this example, if the CIO's designee is the subject of the monitoring, the CIO may conduct the determination.

B. If monitoring without notice is contingent on a determination by CUNY's CIO or their designee, and CUNY's CIO is the subject of the monitoring, such determination shall be made to the University's Executive Vice Chancellor and Chief Operating Officer. In this example, if the CIO's designee is the subject of the monitoring the CIO may conduct the determination.

C. If the subject of the monitoring without notice is a College President, all monitoring without notice determinations assigned to the College President shall be made by the Chancellor.

D. If the monitoring or inspection of an account or activity requires physical entry into a faculty member's office, CUNY reserves the right to enter the faculty member's office without notice to inspect an account and/or to remove applicable CUNY Digital Assets and Resources. The University recognizes the importance of a faculty member's presence under this section D. If exigent circumstances exist requiring the University to enter the faculty member's office without the faculty member's presence, CUNY will consult and notify the Chair of the University Faculty Senate (or Vice Chair if the Chair is unavailable) in a timely manner before the entry and specify the CUNY Digital Assets and Resources to be accessed and/or removed from the faculty member's office.

iii. <u>Other Disclosure.</u>

A. CUNY, in its discretion, may disclose the results of any general or individual monitoring or inspection to appropriate CUNY 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 under FOIL, CUNY may be required to disclose to the public communications made by means of CUNY Digital Assets and Resources whether in conjunction with university business or as personal use.

C. Any disclosures of activity of accounts of individual Users to persons or entities

outside of CUNY, except when required by law, shall be approved by the Senior Vice Chancellor for Legal Affairs and General Counsel, be conducted in accordance with any applicable law, and the CUNY employees subject to such disclosures shall be informed promptly after the disclosure of the actions taken and the reasons for them.

iv. Approval by OGC. In addition to any other approvals required by subsection IV.3.c., any disclosures of activity of accounts of individual Users to persons or entities outside of CUNY, whether discretionary or required by law, is subject to approval by OGC, and shall be conducted in accordance with any applicable law.

v. Annual Statement. OGC shall maintain an annual statement of the instances of account monitoring or inspection that fall within categories D through G above. The statement shall indicate the name of the campus, the reason/cause for each search and the number of such instances. No personally identifiable data shall be included in this statement.

vi. CUNY's Website Privacy Policy. See CUNY's Website Privacy Policy for additional information regarding data collected by CUNY from visitors to the CUNY website at www.cuny.edu.

3. Enforcement.

a. CUNY has the right to temporarily suspend computer use privileges and to remove from CUNY Digital Assets and Resources material it believes violates this policy, pending the outcome of an investigation of misuse or finding of violation. This power may be exercised only by the President of each college or the Chancellor after consultation with OGC.

b. Violation of this policy may result in suspension or termination of an individual's right of access to CUNY Digital Assets and Resources, disciplinary action by appropriate CUNY authorities, referral to law enforcement authorities for criminal prosecution, and/or other legal action, including action to recover civil damages and penalties.

c. Violations will normally be handled through the University disciplinary procedures applicable to the relevant User. For example, alleged violations by students will normally be investigated, and any penalties or other discipline will normally be imposed by the College Office of Student Affairs.

d. Allegations of corruption, fraud, criminal activity, conflicts of interest or abuse that involve CUNY Digital Assets and Resources will be investigated by OGC and any other entity that it deems appropriate, and may result in the notification of external City, State and Federal entities, including the Offices of the New York State Inspector General.

4. Additional Rules. CUNY may adopt additional rules, guidelines and/or restrictions for specific Digital Assets and Resources including computers, systems, networks, or data, or at specific computer facilities at the discretion of the directors of those facilities, provided that these additional rules, policies, guidelines, and/or restrictions comply with this policy.

V. MISCELLANEOUS

1. Waiver of Policy.

a. A CUNY employee or student may apply to the Senior Vice Chancellor for Legal Affairs and General Counsel for an exception or waiver from one or more of the provisions of this policy. Such an application may be for a single use or for periodic or continuous uses, such as in connection with a course or program. Any application for a waiver should be made prior to using the particular CUNY Digital Resource and Assets for the purposes described in the application.

b. The General Counsel & Senior Vice Chancellor for Legal Affairs shall consult with CUNY's CIO and the President of the applicant's College (or, if the applicant is a Central Office employee, the Chancellor), prior to making a determination regarding the application.

c. Users should be aware that CUNY cannot waive federal, state, and/or local law; for example, the contents of CUNY Digital Assets and Resources (including confidential research information) may be subject to a valid subpoena regardless of the terms of any waiver.

2. Disclaimer

a. CUNY shall not be responsible for any damages, costs, or other liabilities of any nature whatsoever regarding the use of CUNY Digital Assets and Resources, except to the extent required by law. This includes, but is not limited to, damages caused by unauthorized access to CUNY Digital Assets and Resources, data loss, or other damages resulting from delays, non-deliveries, or service interruptions, whether or not resulting from circumstances under the CUNY's control.

b. CUNY makes no warranties (expressed or implied) with respect to the use of CUNY Digital Assets and Resources. CUNY accepts no responsibility for the content of web pages or graphics from sources external to CUNY that are linked from CUNY web pages, for any advice or information received by a User through use of CUNY Digital Assets and Resources, or for any costs or charges incurred by a User as a result of seeking or accepting such advice or information.

3. Review of Policy. CUNY reserves the right to change this policy and other related policies at any time. CUNY reserves any rights and remedies that it may have under any applicable law, rule, or regulation. Nothing contained in this policy will in any way act as a waiver of such rights and remedies. The OGC, Office of Academic Affairs, and CIS will conduct periodic reviews of this Policy as necessitated by events or changes in laws and enforcement practices. The foregoing offices in this paragraph will endeavor to conduct a full review of this policy every five (5) years.

4. Examples of Laws and Procedures.

a. Examples of federal and state laws that may apply to the use of CUNY Digital Assets and Resources include those addressing defamation, invasion of privacy, obscenity, child pornography, online gambling, as well as, but not limited to, the following:

Computer Fraud and Abuse Act
Copyright Act of 1976
Electronic Communications Privacy Act
Export control regulations issued by the U.S. Departments of Commerce, State and Treasury

Family Educational Rights and Privacy Act
Federal Trade Commission Safeguards Rule
Freedom of Information Law ("FOIL")
New York State Law with respect to the confidentiality of library records, Civil Practice Law & Rules § 4509
New York State and City technology laws
Health Insurance Portability and Accountability Act of 1996 ("HIPPA")

b. Examples of CUNY rules and policies that may apply to the use of CUNY Digital Assets and Resources include, but are not limited to, those listed below. Other rules and policies may be found in the Manual of General Policy and on the CUNY website:

Gramm- Leach-Bliley Information Security Program
IT Security Policies & Procedures
Policy on Maintenance of Public Order (the "Henderson Rules")
Policy on Sexual Misconduct
CUNY Policy on Academic Integrity
Web Site Privacy Policy
CUNY Policy on Drugs and Alcohol

VI. DEFINITIONS

1. "Business Continuity" refers to CUNY's strategy to ensure that its business operations remain functional and to prevent any risks to the continuation of its business operations when a User is not available or has separated from CUNY.
2. "College" means the University offices (Central Office), each college, school, and other constituent units of the University.
3. "CUNY Digital Assets and Resources" refers to all CUNY owned, licensed, or managed hardware, software, cloud solutions and the tools and processes that integrate with those systems, the data that is created by or resides in these systems and the applications they support. This includes, but is not limited to, desktop and laptop computers, mobile devices that allow or are capable of storing and transmitting information (e.g., cell phones, tablets), computer systems, unified communications and telephony solutions, servers, software, network facilities, databases, memory, memory sticks, portable hard drives and associated peripherals and software. This definition includes the use of these resources on the network via a virtual, physical, or wired or wireless, connection regardless of the ownership of the device connected to the network.
4. "FOIL" is the New York State Freedom of Information Law.
5. "Law" means that all applicable laws, regulations, rules, orders, requirements, and the like, including common law of federal, state, and local governments, courts, governmental authorities, legislative bodies, boards, agencies, commissions, and the like.
6. "Non-Public University Information" ("NPUI") is University Confidential or Sensitive Data as detailed in the Data Classification Standard set forth in CUNY's IT Security Policies and Procedures found at security.cuny.edu. Broadly, NPUI comprises any University Data whose unauthorized disclosure is protected by law or that could result in risk to the University or its users. Some examples of NPUI include, but are not limited to,

the following:

- Personally identifiable information (e.g., Social Security number, driver's license number)
- Financial account, payment card information and credit or debit card number
- Personally identifiable education record
- Protected health information
- Citizenship status
- Personnel record
- Restricted and personally identifiable research data.
- Any other information available in university files and systems that by its nature should be treated confidentially.

7. "OGC" When the term OGC is used concerning authority, approvals, consultations, determinations, or other duties or responsibilities, such reference shall be to the General Counsel or the Deputy General Counsel.
8. "President" means the chief executive officer of any constituent CUNY college or school, including a president or a dean as well as any acting or interim president or dean approved by the Board of Trustees.
9. "Student" is defined as a person who is matriculated and enrolled in courses creditable toward a degree or a certificate approved and registered with the New York State Education Department. This definition applies to undergraduate and graduate students and includes degree and certificate programs that are offered in an on-campus, hybrid, and online format.
10. "User" means anyone who uses CUNY Digital Assets and Resources, including but not limited to, all full-time and part-time CUNY employees and students, CUNY alumni (whether the individual received a degree or completed a program), other individuals working at CUNY such as contractors and RF employees, and visitors to CUNY campuses and facilities. To the extent that the University's collective bargaining agreements grant specific categories of retirees the right to access CUNY Digital Assets and Resources, those retirees will be included in the definition of user.

(Board of Trustees Minutes, 2012, 06-25, 5-B; Amended: Board of Trustees Minutes, 2015, 06-29, 5-A; Amended: Board of Trustees Minutes, 2024, 2-13, 4-B)