Queens College Information Technology Standard	No: PR.AT.1.1 Acceptable Use of Information Technology Resources
IT Standard: **Acceptable Use of Information Technology Resources Policy**	**Updated: 9/27/2022** **Issued By: Queens College, Chief Information Security Officer** **Owner: Queens College Information Technology Services**

1.0 Purpose and Benefits

Appropriate organizational use of information and information technology ("IT") resources and effective security of those resources requires the participation and support of the organization's workforce ("users"). Inappropriate use exposes the organization to potential risks, including virus attacks, compromised network systems and services compromise, and legal issues.

Queens College's computer resources are dedicated to the support of the College's mission of education, research, and public service. In furtherance of this mission, Queens College respects upholds, and endeavors to safeguard the principles of academic freedom, freedom of expression and freedom of inquiry.

Queens College recognizes that there is a concern among the University community that because information created, used, transmitted or stored in electronic form is by its nature susceptible to disclosure, invasion, loss, and similar risks, electronic communications and transactions will be particularly vulnerable to infringements of academic freedom. Queens College's commitment to the principles of academic freedom and freedom of expression includes electronic information. Therefore, whenever possible, Queens College will resolve doubts about the need to access Queens College's Computer Resources in favor of a user's privacy interest.

However, the use of Queens College Computer Resources, including for electronic transactions and communications, like the use of other University-provided resources and activities, is subject to the requirements of legal and ethical behavior. This policy is intended to support the free exchange of ideas among members of the Queens College community and between the Queen's College community and other communities, while recognizing the responsibilities and limitations associated with such exchange.

2.0 Authority

- **Responsible Office(s):** Queens College Information Technology Services & Queens College General Counsel
- **Responsible Executive(s)**: General Counsel
- **Responsible Officer(s)**: Chief Information Security Officer

3.0 Scope

This is a college-wide policy and includes requirements that must be followed if Queens College is to protect the information that is collected in the standard process of business. This policy is to be an additional layer of security on top of existing CUNY security policies and is not intended to or able to supersede CUNY policies.

This policy encompasses all systems, automated and manual, for which Queens College has administrative responsibility, including systems managed or hosted by third parties on behalf of Queens College. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

4.0 Information Statement

Rules for Use of Queens College Computer resources

1. Authorization
    a. Users may not access a Queens College Computer Resource without authorization or use it for purposes beyond the scope of authorization. This includes attempting to circumvent Queens College Computer Resource system protection facilities by hacking, cracking or similar activities, accessing or using another person's computer account, and allowing another person to access or use the User's account.
    b. Notwithstanding subsection 1.a. above, a User may authorize a colleague or clerical assistant to access information under the User's account on the User's behalf while away from a Queens College campus or when the User is unable to efficiently access the information on the User's own behalf (including as a result of a disability), but delegated access will be subject to the rules of Section 10 – Security, below.
    c. Queens College Computer Resources may not be used to gain unauthorized access to another computer system within or outside of Queens College. Users are responsible for all actions performed from their computer account that they permitted or failed to prevent by following ordinary security precautions. QUEENS COLLEGE advisories and resources are available at security.cuny.edu.
2. Purpose
    a. Use of Queens College Computer Resources is generally limited to activities relating to the performance by Queens College employees of their duties and responsibilities, by students in connection with their college courses and activities, and by retired Queens College teaching faculty, librarians, and other retired employees approved by the college president or where the employee is a member of the Central Office staff then by the Chancellor or his or her designee. For example, use of Queens College Computer Resources for private commercial or not-for-profit business purposes, for private advertising of products or services, or for any activity meant solely to foster personal gain, is prohibited. Similarly, use of Queens College Computer Resources for partisan political activity is also prohibited.

b. Except with respect to Queens College employees other than faculty, where a supervisor has prohibited it in writing, incidental personal use of Queens College Computer Resources is permitted so long as such use does not interfere with Queens College operations, does not compromise the functioning of Queens College Computer Resources, does not interfere with the User's employment or other obligations to Queens College, and is otherwise in compliance with this policy, including subsection 2.a. above. Users should be aware that personal messages, data and other information sent or received through a User's Queens College account or otherwise residing in a Queens College Computer Resource are subject to Queens College review pursuant to Section 13 of this policy and may also be subject to public disclosure pursuant to FOIL.

3. Compliance with Law.
    a. Queens College Computer Resources may not be used for any purpose or in any manner that violates Queens College rules, regulations or policies, or federal, state or local law. Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those other 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 their particular use.
    b. Examples of applicable federal and state laws include those addressing defamation, invasion of privacy, obscenity and child pornography, and online gambling, as well as the following:
        i. Computer Fraud and Abuse Act
        ii. Copyright Act of 1976
        iii. Electronic Communications Privacy Act
        iv. Export control regulations issued by the U.S. Departments of Commerce, State and Treasury
        v. Family Educational Rights and Privacy Act
        vi. FOIL
        vii. New York State Law with respect to the confidentiality of library records
    c. Examples of applicable Queens College rules and policies include those listed below. Other rules and policies may be found in the Manual of General Policy and on the Queens College Legal Affairs website:
        i. Gramm-Leach-Bliley Information Security Program
        ii. IT Security Policies & Procedures
        iii. Policy on Maintenance of Public Order (the "Henderson Rules") Sexual Harassment Policy
        iv. University Policy on Academic Integrity
        v. Web Site Privacy Policy
4. Licenses and Intellectual Property.
    a. Users may use only legally obtained, licensed data or software and must comply with applicable licenses or other contracts, as well as copyright, trademark and other intellectual property laws.

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. Protected material may include, among other things, text, photographs, audio, video, graphic illustrations, and computer software. Additional information regarding copyright and file sharing is available on the Queens College Legal Affairs website.

5. False Identity and Harassment.
    a. Users may not employ a false identity, mask the identity of an account or computer, or use Queens College Computer Resources to engage in abuse of others, such as sending harassing, obscene, threatening, abusive, deceptive, or anonymous messages within or outside Queens College.
6. Confidentiality.
    a. Users may not invade the privacy of others by, among other things, viewing, copying, redistributing, posting such data to the Internet, modifying or destroying data or programs belonging to or containing personal or confidential information about others, without explicit permission to do so.
    b. Queens College employees must take precautions by following all IT Security Policies and Procedures to protect the confidentiality of Non-Public University Information encountered in the performance of their duties or otherwise.
7. Integrity of Computer Resources.
    a. Users may not install, use or develop programs intended to infiltrate or damage a Queens College 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 Queens College Computer Resources that they are not sure are safe or may cause excess strain.
8. Disruptive Activities.
    a. Queens College 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;
        ii. spamming, junk mail or other unsolicited mail that is not related to Queens College business and is sent without a reasonable expectation that the recipient would welcome receiving it;
        iii. the inclusion on e-mail lists of individuals who have not requested membership on the lists, other than the inclusion of members of the

Queens College community on lists related to Queens College business; and

iv. downloading of large videos, films or similar media files for personal use.

b. Queens College has the right to require Users to limit or refrain from other specific uses if, in the opinion of the IT director at the User's college, such use interferes with efficient operations of the system, subject to appeal to the President or, in the case of central office staff, to the Chancellor.

9. Queens College Names and Trademarks.
    a. Queens College names, trademarks and logos belong to the University and are protected by law. Users of Queens College Computer Resources may not state or imply that they speak on behalf of Queens College or use a Queens College name, trademark or logo without authorization to do so. Affiliation with Queens College does not, by itself, imply authorization to speak on behalf of Queens College.
    b. Notwithstanding subsection 9.a. above, Queens College employees and students may indicate their Queens College affiliation on e-mail, 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.
10. Security.
    a. Queens College employs various measures to protect the security of its computer resources and of Users' accounts. However, Queens College cannot guarantee such security. Users 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 following Queens College's IT 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 User's college.
11. Filtering.
    a. Queens College reserves the right to install spam, anti-malware, and spyware filters and similar devices if necessary in the judgment of Queens College's Office of Information Technology or a college IT director to protect the security and integrity of Queens College Computer Resources. Queens College 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.
    a. Principal investigators and others who use Queens College 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 confidential research information from unauthorized

access or modification. In general, this means storing the information on a computer or auxiliary hard drive that provides 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. Robust encryption and passwords must be used to protect Non-Public University Information, and is strongly recommended for information stored electronically on all computers, especially portable devices such as notebook computers, Personal Digital Assistants (PDAs), and portable data storage (e.g., auxiliary hard drives, memory sticks) that are vulnerable to theft or loss, as well as for information transmitted over public networks. Software and protocols used should be reviewed and approved by Queens College's Office of Information Technology. In addition, the steps taken to protect such confidential research information should be included in submissions to the Queens College Institutional Review Board reviewing the research protocol.

13. Queens College Access to Computer Resources.
    a. Copying
        i. Queens College may copy a User's account and/or hard drive on a Queens College Computer Resource, without monitoring or inspecting the contents of such account and/or hard drive, at any time for preservation of data or evidence, without notice to the User.
    b. General Monitoring Practices.
        i. Queens College does not routinely monitor, inspect, or disclose individual usage of Queens College Computer Resources without the User's consent. In most instances, if the University needs information located in a Queens College Computer Resource, it will simply request it from the author or custodian. However, Queens College 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. Nevertheless, because of the inherent vulnerability of computer technology to unauthorized intrusions, Users have no guarantee of privacy during any use of Queens College computer resources or in any data in them, whether or not a password or other entry identification or encryption is used. Users may expect that the privacy of their electronic communications and of any materials stored in any Queens College Computer Resource dedicated to their use will not be intruded upon by Queens College except as outlined in this policy.
    c. Monitoring without Notice.
        i. Categories. Queens College may specifically monitor or inspect the activity and accounts of individual users of Queens College computer

resources, including individual login sessions, e-mail and other communications, without notice, in the following circumstances:

1. when the User has voluntarily made them accessible to the public, as by posting to Usenet or a web page.
2. when it is reasonably necessary to do so to protect the integrity, security, or functionality of Queens College or other computer resources, as determined by the college chief information officer or his or her designee, after consultation with Queens College's chief information officer or his or her designee;
3. when it is reasonably necessary to diagnose and resolve technical problems involving system hardware, software, or communications, as determined by the college chief information officer or his or her designee, after consultation with Queens College's chief information officer or his or her designee.
4. when it is reasonably necessary to determine whether Queens College may be vulnerable to liability, or when failure to act might result in significant bodily harm, significant property loss or damage, or loss of evidence, as determined by the college president or a vice president designated by the president or, in the case of the Central Office by the Chancellor or his or her designee, after consultation with the Office of General Counsel and the Chair of the University Faculty Senate (if a current Queens College faculty member's account or activity is involved) or Vice Chair if the Chair is unavailable;
5. when there is a reasonable basis to believe that Queens College policy or federal, state or local law has been or is being violated, as determined by the college president or a vice president designated by the president or, in the case of the Central Office by the Chancellor or his or her designee, after consultation with the Office of General Counsel and the Chair of the University Faculty Senate (if a current Queens College faculty member's account or activity is involved) or Vice Chair if the Chair is unavailable;
6. when an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns, as determined by the college president or a vice president designated by the president and the college chief information officer or his or her designee or, in the case of the Central Office by the Chancellor or his or her designee, after consultation with Queens College's chief information officer or his or her designee, the Office of General Counsel, and the Chair of the University Faculty Senate (if a current Queens College faculty member's account

or activity is involved) or Vice Chair if the Chair is unavailable; or

7. as otherwise required by law.

ii. Procedures. In those situations in which the Chair of the University Faculty Senate is to be consulted prior to monitoring or inspecting an account or activity, the following procedures shall apply:
    1. if the monitoring or inspection of an account or activity requires physical entry into a faculty member's office, the faculty member shall be advised prior thereto and shall be permitted to be present to observe, except where specifically forbidden by law; and
    2. the college president or the Chancellor, as the case may be, shall report the completion of the monitoring or inspection to the Chair and the Queens College employee affected, who shall also be told the reason for the monitoring or inspection, except where specifically forbidden by law.

iii. Other Disclosure.
    1. Queens College, in its discretion, may disclose the results of any general or individual monitoring or inspection to appropriate Queens College 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.
    2. In addition, users should be aware that Queens College may be required to disclose to the public under FOIL communications made by means of Queens College Computer Resources whether in conjunction with University business or as incidental personal use.
    3. Any disclosures of activity of accounts of individual Users to persons or entities outside of Queens College, 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, Queens College employees subject to such disclosures shall be informed promptly after the disclosure of the actions taken and the reasons for them.

iv. Annual Statement. The Office of General Counsel shall issue an annual statement of the instances of account monitoring or inspection that fall within categories D through G above. The statement shall indicate the number of such instances and the cause and result of each. No personally identifiable data shall be included in this statement.

v. Privacy Policy. See Queens College's Web Site Privacy Policy for additional information regarding data collected by Queens College from visitors to the Queens College website at www.cuny.edu.

14. Waiver of Policy
    a. A Queens College employee or student may apply to the General Counsel for an exception or waiver from one or more of the provisions of this policy. Such 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 Queens College Computer Resource for the purposes described in the application.
    b. The written waiver application must state:
        i. the policy provision or provisions for which the User is seeking a waiver;
        ii. how the User plans to use Queens College Computer Resource to be covered by the waiver and the reasons why the User believes a waiver should be approved;
        iii. if the waiver involves confidential research information, what steps will be taken to protect such information;
        iv. 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. The General Counsel shall consult with the Queens College's chief information officer and the president of the applicant's college (or, if the applicant is a Central Office employee, the Chancellor) or their designees, prior to making a determination regarding the application.
    d. Users should be aware that Queens College cannot waive federal, state or local law; for example, the contents of Queens College Computer Resources (including confidential research information) may be subject to a valid subpoena regardless of the terms of any waiver.
15. Enforcement.
    a. Violation of this policy may result in suspension or termination of an individual's right of access to Queens College Computer Resources, disciplinary action by appropriate Queens College authorities, referral to law enforcement authorities for criminal prosecution, or other legal action, including action to recover civil damages and penalties.
    b. 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 Office of Student Affairs.
    c. Queens College has the right to temporarily suspend computer use privileges and to remove from Queens College computer 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.
16. Additional Rules. Additional rules, policies, guidelines and/or restrictions may be in effect for specific computers, systems, or networks, or at specific computer facilities at the discretion of the directors of those facilities. Any such rules which potentially limit the privacy or confidentiality of electronic communications or information contained in or delivered by or over Queens College Computer Resources will be subject to the substantive and procedural safeguards provided by this policy.

17. Disclaimer.
    a. Queens College shall not be responsible for any damages, costs or other liabilities of any nature whatsoever with regard to the use of Queens College Computer Resources. This includes, but is not limited to, damages caused by unauthorized access to Queens College Computer Resources, data loss, or other damages resulting from delays, non-deliveries, or service interruptions, whether or not resulting from circumstances under the Queens College's control.
    b. Users receive and use information obtained through Queens College Computer Resources at their own risk. Queens College makes no warranties (expressed or implied) with respect to the use of Queens College Computer Resources. Queens College accepts no responsibility for the content of web pages or graphics that are linked from Queens College web pages, for any advice or information received by a user through use of Queens College Computer Resources, or for any costs or charges incurred by a user as a result of seeking or accepting such advice or information.
    c. Queens College reserves the right to change this policy and other related policies at any time. Queens College 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.

5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer's exception process.

6.0 Definitions of Key Terms

Term	Definition
Queens College Computer Resources	"Queens College Computer Resources" refers to all computer and information technology hardware, software, data, access and other resources owned, operated, or contracted by CUNY. This includes, but is not limited to, desktop and laptop computers, handheld devices that allow or are capable of storing and transmitting information (e.g., cell phones, tablets), mainframes, minicomputers, servers, network facilities, databases, memory, memory sticks, and associated peripherals and software, and the applications they

	support, such as e-mail, cloud computing applications, and access to the internet.
Email	“E-mail” includes point-to-point messages, postings to newsgroups and listservs, and other electronic messages involving computers and computer networks.
Faculty	“Faculty” includes full-time, part-time, and adjunct faculty.
FOIL	“FOIL” is the New York State Freedom of Information Law.
Non-Public University Information	“Non-Public University Information” has the meaning set forth in CUNY’s IT Security Policies and Procedures found at security.cuny.edu, namely: personally identifiable information (such as an individual’s Social Security Number; driver’s license number or 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 access to an individual’s financial account; personal electronic mail address; Internet identification name or password; and parent’s surname prior to marriage); information in 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; other information relating to the administrative, business, and academic activities and operations of the University (including employee evaluations, employee home addresses and telephone numbers, and other employee records that should be treated confidentially); and any other information available in University files and systems that by its nature should be treated confidentially .
User	“User” means a user of Queens College Computer Resources, including all current and former users, whether affiliated with Queens College or not, and whether accessing those resources on Queens College campus or remotely.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:
Chief Information Security Officer
Aaron Wheeler
Aaron.Wheeler@qc.cuny.edu

8.0 Revision History

This policy shall be reviewed at least once every year to ensure relevancy.

Date	Description of Change	Reviewer
9/27/2022	Initial Changes to apply to Queens College	DVogel
03/20/25	Added number convention and control title	AWheeler
	Policy Implemented	

9.0 Related Documents