WAGNER COLLEGE

POLICY:
ACCEPTABLE USE

DOCUMENT #: POL-0003
EFFECTIVE: 05/31/2023
OWNER: ISO

CONTENTS

WAGNER COLLEGE

1.0 PURPOSE

Wagner College's technology infrastructure exists to support the institution and administrative activities needed to fulfill the institution's mission. Access to these resources is a privilege that should be exercised responsibly, ethically and lawfully.

The purpose of this Acceptable Use Policy is to clearly establish each member of the institution's role in protecting its information assets and communicate minimum expectations for meeting these requirements. Fulfilling these objectives will enable Wagner College to implement a comprehensive system-wide Information Security Program.

2.0 SCOPE

This policy applies to all users of computing resources owned, managed or otherwise provided by the institution. Individuals covered by this policy include, but are not limited to all faculty, staff, students , and service providers with access to the institution's computing resources and/or facilities. Computing resources include all Wagner College owned, licensed or managed hardware and software, email domains and related services and any use of the institution's network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

3.0 PRIVACY

Wagner College will make every reasonable effort to respect a user's privacy. However, faculty, staff and students do not acquire a right of privacy for communications transmitted or stored on the institution's resources. Additionally, in response to a judicial order or any other action required by law or permitted by official Wagner College policy or as otherwise considered reasonably necessary to protect or promote the legitimate interests of the institution, the President of the institution may authorize a Wagner College official or an authorized agent, to access, review, monitor and/or disclose computer files associated with an individual's account. Examples of situations where the exercise of this authority would be warranted include, but are not limited to, the investigation of violations of law or the institution's rules, regulations, or policy, or when access is considered necessary to conduct Wagner College business due to the unexpected absence of faculty, staff or students, or to respond to health or safety emergencies.

4.0 POLICY

Activities related to Wagner College's mission take precedence over computing pursuits of a more personal or recreational nature. Any use that disrupts the institution's mission is prohibited.

Following the same standards of common sense, courtesy, and civility that govern the use of other shared facilities, acceptable use of information technology resources generally respects all individuals' privacy but is subject to the right of individuals to be free from intimidation, harassment, and unwarranted annoyance. All users of Wagner College's computing resources must adhere to the requirements enumerated below.

4.1 FRAUDULENT AND ILLEGAL USE

Wagner College explicitly prohibits the use of any information system for fraudulent and/or illegal purposes. While using any of the institution's information systems, a user must not engage in any activity that is illegal under local, state, federal, and/or international law. As a part of this policy, users must not:

- Violate the rights of any individual or institution involving information protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by Wagner College.
- Use in any way copyrighted material including, but not limited to, photographs, books, or other copyrighted sources, copyrighted music, and any copyrighted software for which the institution does not have a legal license.
- Export software, technical information, encryption software, or technology in violation of international or regional export control laws.
- Issue statements about warranty, expressed or implied, unless it is a part of normal job duties, or make fraudulent offers of products, items, and/or services.

Any user that suspects or is aware of the occurrence of any activity described in this section, or any other activity they believe may be fraudulent or illegal, must notify his/her manager immediately.

If any user creates any liability on behalf of Wagner College due to inappropriate use of the institution's resources, the user agrees to indemnify and hold the institution harmless, should it be necessary for Wagner College to defend itself against the activities or actions of the user.

4.2 CONFIDENTIAL INFORMATION

Wagner College has an ethical and legal responsibility for protecting confidential information per its Data Classification Policy. To that end, there are some general positions that the institution has taken:

- Transmission of confidential information by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.) is prohibited.
- The writing or storage of confidential information on mobile devices (phones, tablets, USB drives) and removable media is prohibited. Mobile devices that access confidential information will be physically secured when not in use and located to minimize the risk of unauthorized access.

- All faculty, staff, students, and service providers will use approved workstations or devices to access the institution's data, systems, or networks. Non-institution-owned workstations that store, process, transmit, or access confidential information are prohibited. Accessing, storage, or processing confidential information on home computers is prohibited.
- All institution portable workstations will be securely maintained when in the possession of a faculty, staff or student member. Such workstations will be handled as carry-on (hand) baggage on public transport. They will be concealed and/or locked when in private transport (e.g., locked in the trunk of an automobile) when not in use.
- Photographic, video, audio, or other recording equipment will not be utilized in secure areas.
- All confidential information stored on workstations and mobile devices must be encrypted.
- All faculty, staff, and students who use institution-owned workstations will take all reasonable precautions to protect the confidentiality, integrity, and availability of information contained on the workstation.
- Institution faculty, staff, students, and affiliates who move electronic media or information systems containing confidential information are responsible for the subsequent use of such items and will take all appropriate and reasonable actions to protect them against damage, theft, and unauthorized use.
- Institution faculty, staff, and students members will activate their workstation locking software whenever they leave their workstation unattended or will log off from or lock their workstation when their shift is complete.

4.3 HARRASSMENT

Wagner College is committed to providing a safe and productive environment, free from harassment, for all faculty, staff, and students. For this reason, users must not:

- Use of institution information systems to harass any other person via e-mail, telephone, or any other means.
- Actively procure or transmit material that is in violation of sexual harassment or hostile workplace laws.

If a user feels that they are being harassed through the use of the institution's information systems, the user must report it, in writing, to their instructor or any department head.

Harassment via electronic means, also known as cyberbullying or online harassment, is a serious issue that can have a significant impact on individuals and communities within a college campus. This type of harassment can take many forms, including but not limited to, unwanted emails, text messages, social media posts, and online comments.

Report the incident: The first step in addressing harassment via electronic means is to report the incident to the appropriate authorities. This may include campus security, the dean of students,

or the Title IX coordinator. These individuals can provide guidance and support in addressing the situation and taking appropriate action.

Document the incident: It is important to document any incidents of harassment, including the date, time, and nature of the incident. This can help to provide evidence of the harassment and can be useful in any subsequent investigations.

Seek support: Harassment can be a traumatic experience, and it is important to seek support from friends, family, or a counselor. Many colleges have counseling services available to students and staff, and these services can provide a safe and confidential space to talk about the experience and receive support.

Take steps to protect yourself: If you are experiencing harassment via electronic means, it is important to take steps to protect yourself. This may include blocking the individual who is harassing you, changing your phone number or email address, or increasing your privacy settings on social media.

Harassment via electronic means is a serious issue that can have a significant impact on individuals and communities. By taking action to address the situation and raise awareness of the issue, we can work towards creating a safer and more supportive college campus environment.

4.4 INCIDENT REPORTING

Wagner College is committed to responding to security incidents involving personnel, institution-owned information, or institution-owned information assets. As part of this policy:

- The loss, theft, or inappropriate use of institution access credentials (e.g. passwords, key cards, or security tokens), assets (e.g. laptops, cell phones), or other information will be reported to the IT Service Desk.
- No faculty, staff, or student will prevent another member from reporting a security incident.
- No faculty, staff, or student will prevent a member of the IT Staff from removing infected hardware from premises.

  Incident reporting involving personnel, institution-owned information, or institution-owned information assets typically involves reporting any security incidents or breaches that may compromise the confidentiality, integrity, or availability of such information. This could include:

  Unauthorized access to institution-owned information or systems by personnel or external entities.
  Theft or loss of institution-owned information or assets, including physical theft of devices or data storage media.
  Unintentional disclosure of institution-owned information, such as sending sensitive information to the wrong recipient or sharing it on a public forum.

Malicious actions by personnel, such as intentionally deleting or modifying data or installing malware on institution-owned systems.
Physical damage to institution-owned assets, such as equipment or hardware, resulting in loss of data or system downtime.
Institutions typically have incident response policies and procedures in place to guide personnel on how to report incidents involving institution-owned information and assets.

These policies often include steps for containing the incident, assessing the impact, and notifying appropriate stakeholders. It is important for personnel to report incidents promptly to minimize the potential impact and prevent further damage.

4.5 MALICIOUS ACTIVITY

Wagner College strictly prohibits the use of information systems for malicious activity against other users, the institution's information systems themselves, or the information assets of other parties.

This policy aims to prevent unauthorized access, modification, or destruction of information and information systems. It applies to all users of institution-owned information systems, including employees, contractors, and third-party vendors. Users are prohibited from engaging in any activities that may harm the information systems or data of other users or of Wagner College.

Examples of malicious activities that are prohibited include:

- Unauthorized access to another user's account or information system.
- Installation of malware, viruses, or other harmful software.
- Denial of service attacks that disrupt the availability of information systems or networks.
- Theft or destruction of institution-owned information or assets.
- Phishing or social engineering attacks aimed at obtaining sensitive information.

Violations of the no hacking policy can result in serious consequences, including termination of employment, legal action, and loss of trust and reputation. Therefore, it is crucial for all users of institution-owned information systems to adhere to this policy and report any suspicious or malicious activity immediately.

4.5.1 DENIAL OF SERVICE

Users must not:

- Perpetrate, cause, or in any way enable disruption of Wagner College's information systems or network communications by denial-of-service methods.
- Knowingly introduce malicious programs, such as viruses, worms, and Trojan horses, to any information system.

- Intentionally develop or use programs to infiltrate a computer, computing system, or network and/or damage or alter the software components of a computer, computing system or network.

The policy explicitly prohibits users from perpetrating, causing, or enabling disruption of Wagner College's information systems or network communications by denial-of-service methods. This includes any attempt to overload or flood the network with traffic, rendering it inaccessible or unusable for legitimate users.

Users are also prohibited from knowingly introducing malicious programs, such as viruses, worms, and Trojan horses, to any information system. This can include downloading or installing malicious software, opening suspicious email attachments, or visiting compromised websites.

Finally, users are prohibited from intentionally developing or using programs to infiltrate a computer, computing system, or network and/or damage or alter the software components of a computer, computing system or network. This includes activities such as hacking, cracking, or exploiting vulnerabilities in information systems or networks.

Violations of this policy can result in severe consequences, including suspension of access to information systems, termination of employment or contract, and legal action. Therefore, it is critical for all users to adhere to this policy and report any suspicious or malicious activity immediately.

4.5.2 CONFIDENTIALITY

Users must not:

- Perpetrate, cause, or in any way enable security breaches, including, but not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access;
- Facilitate use or access by non-authorized users, including sharing their password or other login credentials with anyone, including other users, family members, or friends;
- Use the same password for Wagner College accounts as for other non-Wagner College access (for example, personal ISP account, social media, email, etc.);
- Attempt to gain access to files and resources to which they have not been granted permission, whether or not such access is technically possible, including attempting to obtain, obtaining, and/or using another user's password; or
- Make copies of another user's files without that user's knowledge and consent.
- All encryption keys employed by users must be provided to Information Technology if requested, in order to perform functions required by this policy.
- Base passwords on something that can be easily guessed or obtained using personal information (e.g. names, favorite sports teams, etc.).
- Pictures of Wagner College off-limit locations(i.e. data center) are not to be posted on any Social Media Platform.

Additionally, it is important for users to understand the potential consequences of their actions. A breach of security could result in a loss of sensitive or confidential data, a compromise of Wagner College's reputation, and legal and financial liabilities. Sharing login credentials could allow unauthorized access to sensitive data or systems, and installing unauthorized software or hardware could introduce security vulnerabilities into Wagner College's information systems. Attempting to disrupt or degrade the performance of Wagner College's information systems or network could impact the ability of the institution to provide services to its students, faculty, and staff, and could also negatively affect Wagner College's reputation.

By adhering to this policy, users can help to ensure the confidentiality, integrity, and availability of Wagner College's information systems and data, as well as protect the institution's reputation and financial health.

4.5.3 IMPERSONATION

Users must not:

- Circumvent the user authentication or security of any information system.
- Add, remove, or modify any identifying network header information ("spoofing") or attempt to impersonate any person by using forged headers or other identifying information.
- Create and/or use a proxy server of any kind, other than those provided by Wagner College, or otherwise redirect network traffic outside of normal routing with authorization.
- Use any type of technology designed to mask, hide, or modify their identity or activities electronically.

The policy prohibiting the circumvention of user authentication or security, spoofing, using unauthorized proxy servers, and masking identity or activities is critical to maintaining the integrity of Wagner College's information systems and data. These activities can be used to evade detection or gain unauthorized access to information systems or data, and can be detrimental to the security and privacy of Wagner College and its users.

Circumventing user authentication or security measures could allow unauthorized individuals to gain access to information systems or data, potentially leading to data breaches, theft of sensitive information, and legal and financial liabilities. Spoofing or impersonating someone else through the use of forged headers or other identifying information can also lead to confusion, miscommunication, and potential security breaches.

Violations of this policy can result in disciplinary action, up to and including termination of employment or contract, legal action, and criminal prosecution. Therefore, it is critical for all users to adhere to this policy and report any suspicious or unauthorized activity immediately.

4.5.4 NETWORK DISCOVERY

Users must not:

- Use a port scanning tool targeting either Wagner College's network or any other external network, unless this activity is a part of the user's normal job functions, such as a member of the Office of Information Technology, conducting a vulnerability scan, and faculty utilizing tools in a controller environment.
- Use a network monitoring tool or perform any kind of network monitoring that will intercept data not intended for the user, unless this activity is a part of the user's normal job functions.

Unauthorized port scanning and network monitoring can potentially harm the network and user data. Engaging in such activities without proper authorization may be considered unethical or even illegal, as it can breach the security of the network and compromise sensitive information. It is important to prioritize the security and integrity of the network and its users, and to act in accordance with any established policies and guidelines.

4.6 OBJECTIONABLE CONTENT

Wagner College strictly prohibits the use of institutional information systems for accessing or distributing content that other users may find objectionable. Users must not post, upload, download, or display messages, images, sound files, text files, video files, newsletters, or related materials considered to be:

- Political
- Racist
- Sexually-explicit
- Violent or promoting violence

This policy prohibits the use of institutional information systems for accessing or distributing content that other users may find objectionable. Users are not allowed to post, upload, download, or display messages, photos, images, sound files, text files, video files, newsletters, or related materials that are political, racist, sexually explicit, or promoting violence. It is important for users to adhere to this policy to ensure a safe and respectful online environment for all members of the Wagner College community.

Commented [BH1]: Does any exception need to be made for academic research or classwork?

4.7 HARDWARE AND SOFTWARE

Wagner College strictly prohibits the use of any hardware or software that is not purchased, installed, configured, tracked, and managed by the institution. Users must not:

- Install, attach, connect or remove or disconnect, hardware of any kind, including wireless access points, storage devices, and peripherals, to any institution information system without the knowledge and permission of Information Technology.

- Download, install, disable, remove or uninstall software of any kind, including patches of existing software, to any institution information system without the knowledge and permission of the institution.
- Use personal flash drives, or other USB based storage media, without prior approval from their manager.
- Take Wagner College equipment off-site without prior authorization.

The use of unauthorized hardware or software can introduce security risks and vulnerabilities to an organization's information systems. Unapproved hardware or software may not have gone through the same rigorous security testing and implementation processes as authorized hardware and software, making it more susceptible to security breaches, malware infections, and data loss.

Allowing unauthorized hardware and software can also make it more difficult for an organization's IT department to track and manage its technology assets, which can lead to increased maintenance costs and a higher risk of lost or stolen equipment.

By enforcing policies that require the use of authorized hardware and software, an organization can better protect its information systems, reduce the risk of security breaches, and ensure that all technology assets are tracked and managed effectively.

4.8 MESSAGING

The institution provides a robust communication platform for users to fulfill its mission. Users must not:

- Automatically forward electronic messages of any kind, by using client message handling rules or any other mechanism.
- Send unsolicited electronic messages, including “junk mail” or other advertising material to individuals who did not specifically request such material (spam).
- Solicit electronic messages for any other digital identifier (e.g. e-mail address, social handle, etc.), other than that of the poster's account, with the intent to harass or to collect replies.
- Create or forward chain letters or messages, including those that promote “pyramid” schemes of any type.

The communication policies implemented by the institution aim to ensure that the institution's communication platform is used effectively, ethically, and without causing unnecessary disruptions or harassment to other users. By enforcing policies that prohibit these activities, the institution can ensure that its communication platform is used effectively and efficiently for its intended purposes, while also promoting a safe and respectful digital environment for all users.

4.9 REMOTE WORKING

When working remote, user must:

- Be given explicit approval from their immediate supervisor.
- Safeguard and protect any institution-owned or managed computing asset (e.g. laptops and cell phones) to prevent loss or theft.
- Not utilize personally-owned computing devices for Wagner College work, including transferring Wagner College information to personally-owned devices, unless approved by a member of Wagner College IT Staff.
- Take reasonable precautions to prevent unauthorized parties from utilizing computing assets or viewing Wagner College information processed, stored or transmitted on institution-owned assets.
- Not create or store confidential or private information on local machines unless a current backup copy is available elsewhere.
- Not access or process confidential information in public places or over public, insecure networks.
- Only use approved methods for connecting to the institution (e.g. VPN).

The policies regarding remote work aim to ensure that the institution's computing assets and information are protected and secure, even when users are working from outside of the institution's physical premises.

Before working remotely, users must receive approval from their supervisor, which ensures that the work being done remotely aligns with the institution's policies and goals. When working remotely, users must take precautions to protect institution-owned computing assets from loss or theft, which can help prevent unauthorized access to institutional information.

Using personally-owned computing devices for Wagner College work can introduce security risks and vulnerabilities, which is why users are not allowed to do so unless approved by a member of the institution's IT staff. This helps to ensure that institution information is accessed and stored on secure and authorized devices.

Users must also take reasonable precautions to prevent unauthorized parties from accessing institution-owned computing assets or viewing Wagner College information processed, stored, or transmitted on those assets. Additionally, users should not create or store confidential or private information on local machines unless a current backup copy is available elsewhere.

To ensure the security of institutional information, users should not access or process confidential information in public places or over public, unsecured networks. Finally, users should only use approved methods for connecting to the institution, such as VPN, which helps to ensure the security and integrity of institution information while working remotely.

4.9 OTHER

In addition to the other parts of this policy, users must not:

- Stream video, music, or other multimedia content unless this content is required to perform the user’s normal business functions;

- Use the institution's information systems for commercial use or personal gain; or
- Use the institution's information systems to play games or provide similar entertainment.

Commented [BH2]: Do any exceptions need to be made for networks within the student housing areas?

The policies regarding the use of institution information systems for streaming, commercial use, and entertainment aim to ensure that the institution's information systems are used for legitimate business purposes and not for personal gain or entertainment.

Streaming video, music, or other multimedia content can consume significant amounts of bandwidth and may interfere with the institution's network performance. Unless required to perform the user's normal business functions, streaming should be avoided.

Using the institution's information systems for commercial use or personal gain can be seen as a conflict of interest and may violate the institution's code of conduct. The use of institutional resources for personal purposes can also be seen as an abuse of power.

By enforcing policies that prohibit these activities, the institution can ensure that its information systems are used for legitimate business purposes, which helps to maximize productivity and promote an environment focused on achieving the institution's goals.

5.0 ROLES AND RESPONSIBILITIES

Wagner College reserves the right to protect, repair, and maintain the institution's computing equipment and network integrity. In accomplishing this goal, Wagner College IT personnel or their agents must do their utmost to maintain user privacy, including the content of personal files and Internet activities. Any information obtained by IT personnel about a user through routine maintenance of the institution's computing equipment or network should remain confidential unless the information pertains to activities that are not compliant with acceptable use of Wagner College's computing resources.

6.0 ENFORCEMENT

Enforcement is the responsibility of the institution's President or designee. Users who violate this policy may be denied access to the institution resources and may be subject to penalties and disciplinary action both within and outside of Wagner College. The institution may temporarily suspend or block access to an account, prior to the initiation or completion of disciplinary procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of the institution or other computing resources or to protect Wagner College from liability.

Users are subject to disciplinary rules described in the Employee Handbook, and other policies and procedures governing acceptable workplace behavior.

7.0 EXCEPTIONS

Exceptions to the policy may be granted by the Chief of Information Technology, or by his or her designee. All exceptions must be reviewed annually.

8.0 REFERENCES

- The Gramm - Leach Bliley Act (GLBA)
- Family Educational Rights and Privacy Act (FERPA)
- New York State Information Security Breach and Notification Act
- NIST 800-53
- FIPS-199
- PCI DSS 3.1
- New York Civil Practice Law and Rules § 4509
- Code of Ethics of the American Library Association

9.0 RELATED POLICIES

- Information Security Policy
- Data Classification Policy
- Data Classification and Handling Procedure

10.0 RESPONSIBLE DEPARTMENT

[Insert Responsible Department]

11.0 POLICY AUTHORITY

This policy is issued for Wagner College.