WAGNER COLLEGE

INFORMATION TECHNOLOGY

Responsible Use of Technology and Information Resources

Introduction: The policies and guidelines outlined in this document apply to the entire Wagner College community: students, faculty, staff, alumni and friends of Wagner College. The use of any computer, telephony or network resource of Wagner College constitutes agreement to be bound by these policies. These policies and guidelines are subject to change as technology and state and federal laws develop and change. Suggestions or comments on these policies are welcomed and should be sent to the Chief Information Officer.

Policies contained in this document

I. Responsible Use of Information and Computing Resources
II. Information Security and Privacy
III. Email and Voicemail Guidelines
IV. Protecting Intellectual Property and Copyright
V. Problem Resolution and Policy Violation
VI. Reporting Abusive Incidents, Harassment or Irresponsible Behavior Related to Technology

I. Responsible Use of Information and Computing Resources

All members of the Wagner College community who use the College's computing and network facilities need to use them in an ethical, responsible and legal manner. This means that individuals are personally responsible for their use of these resources and must be familiar with and follow the policies below. An attempt to engage in a prohibited activity is considered a violation whether the attempt is successful or not.

The Wagner College network and computer infrastructure is a critical and finite resource. Community members rely on high availability and good performance to accomplish their work. Systems using excessive amounts of bandwidth, causing network disruption or that are deemed to be a security and/or privacy risk may be taken off the network or be otherwise limited without warning. Information Technology may employ automated systems that partition or restrict network bandwidth, protocols, or access either internally or at the Internet gateway.

Wagner College provides computers, software, and network equipment for use by the College community. The College retains ownership and reserves the right to add, remove, upgrade and replace hardware and software on those systems as deemed necessary by

Information Technology.

Computers in residence halls must be registered with Wagner College before they will be allowed to access the Wagner College network. The registrant is responsible for all network activity originating from the registered computer regardless of the individual operating the computer, either directly or remotely. All network activity originating from the computer must follow the policies outlined in this document.

Members of the Wagner College community must:

• Use resources supplied for purposes which are consistent with the business and mission of Wagner College.
• Use the College's computing facilities and information resources, including hardware, software and computer accounts, responsibly and appropriately.
• Respect the rights and property of others.
• Comply with all applicable federal, state, and local laws and College policy. Comply with all contractual and license agreements.
• Accept personal responsibility for the proper use of individual accounts and all activity associated with them.
• Follow all posted and published policies when using all computer laboratories and classrooms.

Members of the Wagner College community may not:

• Share accounts, passwords or other computer or network authentication. Information Technology staff may create group or organization accounts when there is a need.
• Use any means to view or intercept data or network traffic not intended for their viewing or use.
• View, copy, disclose or modify any files or data that do not belong to them, or to which they do not have specific permission.
• Use computing or network resources to harass, threaten or otherwise cause harm to others.
• Use the College's computing resources for commercial purposes not related to the academic, research, and scholarly mission of the College.
• Use any IT system in a way which suggests College endorsement of any political party, candidate or ballot initiative. This includes e-mailing political messages to any list service maintained by the College which is not explicitly purposed for the posting of political messages and including such messages in your signature.
• Interfere with the proper functioning of the Wagner College wired or wireless network. In particular, users may not perform service denial attacks and users may not install their own wireless access points on campus.
• Use Wagner College IT systems to store, distribute, produce, publish and/or sell obscene, copyrighted, or otherwise illegal content. Content found to resemble these characteristics is subject to deletion without notice.

II. Information Security and Privacy

The College takes information security and privacy very seriously for all of its members and all of its systems.

Members of the Wagner College community must:

• Be personally responsible for the security and usage of any system connected to the Wagner College network that is not owned by Wagner College.
• Choose passwords that meet College standards and keep your passwords secure.
• Report unauthorized use of your accounts to your supervisor or to Information Technology. If you discover a possible security issue related to a College system, report the problem immediately to Information Technology.
• Use only those computers and computer accounts for which you have authorization. If you need additional privileges or access, contact your supervisor.
• Handle personally identifiable, sensitive or confidential data and files with the utmost care and explicitly adhere to FERPA rules, where appropriate.
• Comply with requests from Information Technology. The Information Technology staff will conduct periodic security checks on systems and networks. Individuals may be asked to change their password, upgrade software, apply a patch or perform some other action to improve system security. Non-compliance may result in access termination.
• Respect the rights, property and privacy of others.

Members of the Wagner College community may not:

• Disguise or attempt to disguise their identity or the identity of their account or the machine that they are using. Users may not attempt to impersonate another person or identity.
• Attempt to gain unauthorized access to any account or system.
• Copy, report or distribute any personally identifiable, sensitive or confidential data or files to which you as a user of College resources are not authorized or gain inadvertent access. Users must report any occurrences to the data owner.

The foregoing is not an all-inclusive list; the College reserves the right to determine what uses of its equipment and facilities fall within the bounds of the business and mission of the College. Report abuses of information or computing resources to Information Technology.

Email and Voicemail Guidelines

Email is the official method of communication for Wagner College and all official communication will be sent to the individual's Wagner email address. All students, faculty and staff must check their Wagner email on a regular basis. The only exception to this rule is when a communication contains confidential information or sensitive data. Neither email nor voicemail should be used for confidential

communication or the transmission of sensitive data. All Wagner College email addresses are owned by Wagner College.

Wagner College email is powered by Google Apps. Usage is also subject to Google Policies and Terms of Service.

Google Terms of Service:
http://www.google.com/intl/en/policies/terms/

Google Policies on the Products:
https://support.google.com/accounts/answer/147806

Email and voicemail will be kept as private as possible, but Wagner College may access email and voicemail records when it has a legitimate business reason to do so. The President, or his/her designate, will determine what constitutes a legitimate business reason. In the normal course of managing the servers and the network, Information Technology staff may see your content. Administrators and Information Technology professionals will not read email that is not addressed to them nor listen to someone else's voicemail messages unless necessary in the course of their duties. Be aware that email that is improperly addressed may be delivered to an unintended recipient. Email that cannot be delivered may be directed to system administrators. The contents of an email message can easily be copied or redistributed by the recipient. Information Technology cannot guarantee that all email and voicemail will remain private.

E-mail and voicemail messages are records that could be subject to review with just cause. All information in electronic form on central computers can be subpoenaed. Messages that the user has deleted may still exist on system's backup media for weeks or months. Certain types of email and voicemail and their uses are prohibited. These include, but are not limited to, chain letters, obscene messages, harassing messages, and unsolicited political messages. Email or voicemail that violates any College policy or is otherwise used for an illegal purpose is prohibited.

All email sent through the College's systems and network must accurately show from whom the email originated.

The College employs automated systems to reduce the amount of unwanted 'junk' mail or spam. It is known that this may on occasion reject a valid e-mail.

III. Protecting Intellectual Property and Copyright

Copyright is a form of protection of intellectual property provided by the laws of the United States to the authors of original works. Copyright is an issue of particular seriousness because technology now allows the easy copying and transmission of some protected works.

It is the responsibility of all students, faculty, and staff at Wagner College to understand and comply with the College's copyright policy.

The College's designated agent for notices under the Digital Millennium Copyright Act is the Dean of the Library.

Federal copyright laws also protect the software available for use on computers at Wagner College. The software provided through the College for use by faculty, staff, and students may be used only on computing equipment as specified in the various software licenses.

Faculty, staff, or students must not copy or reproduce any licensed software or intellectual property found on College computing equipment, except as expressly permitted by the software license, author, or granting authority. Faculty, staff, and students may not use unauthorized copies of licensed software on College-owned computers.

IV. Problem Resolution and Policy Violations

In cases where a member of the College community has allegedly committed a policy violation, broken a law, or is causing harm to the information infrastructure, Information Technology may immediately revoke access privileges pending the outcome of a full review of the problem. In such cases, the individual will be notified as quickly as possible, by phone, electronic, campus or U.S. mail of the alleged violation. A representative of the Information Technology staff will contact the person to propose a meeting to discuss the alleged violation.

Depending on the nature of the alleged offense, Information Technology may contact the appropriate senior college official (unit Vice President, Provost, Dean of the College) or law enforcement agency alerting them of the alleged violation and conferring with them on the appropriate next steps. If the problem or issue in question overlaps with another disciplinary or law enforcement process, Information Technology will coordinate with the appropriate office or agency. Information Technology will fully cooperate with the authorities to provide any information necessary for the litigation process. Penalties for illegal activity or serious violations may be as severe as suspension or dismissal from the College or criminal prosecution.

Compromised e-mail accounts may locked out by Information Technology until the situation has been fully investigate and resolved. Accounts which were compromised malicious activity by the user would be allowed to regain access to their account once Information Technology has completed its duties to secure the account (which includes, but not limited to, setting a "strong" password, removal of e-mail filters, forwards, as well as non-Google apps associated with the account). Users who participated in malicious activities will not get their accounts back and disciplinary actions will be taken as specified above.

V. Reporting Abusive Incidents, Harassment or Irresponsible Behavior Related to Technology

If you are a victim of abusive incidents related to technology or you become aware of abusive use of College technology resources, report the violation to your supervisor or the Chief Information Office. Keep copies of e-mail messages, a record of the time and date(s) of the occurrence, and all other information related to the incident for investigative purposes.