



THE NEW SCHOOL

Information Resource Acceptable Use Policy

**Revision 1.0
November 18, 2011**



TABLE OF CONTENTS

1	INTRODUCTION	1
1.1	Objective	1
1.2	Scope.....	1
1.3	Compliance	2
1.3.1	Monitoring.....	2
1.3.2	Enforcement.....	2
1.4	Exceptions.....	3
2	GENERAL POLICY ON ACCEPTABLE USE.....	5
2.1	Personal Use of University Information Resources.....	5
2.2	Storage of Personal Data on University Computers.....	6
2.3	Connection to University Networks	6
2.4	Reporting Security Incidents	6
2.5	Prohibited and Inappropriate Use	7
2.5.1	Excessive Non-Priority Use of Information Resources	7
2.5.2	Unacceptable System and Network Activities.....	7
2.5.3	Unauthorized Use of Intellectual Property.....	8
2.5.4	Inappropriate or Malicious Use of IT Systems	8
2.5.5	Misuse of E-Mail and Communications Activities	9
3	ACCEPTABLE USE OF ADMINISTRATIVE INFORMATION RESOURCES	11
3.1	Information Ownership and Classification.....	11
3.2	Maintaining the Security of Classified Information	11
3.3	Use of Administrative Computers.....	12
4	PRIVILEGED USER CODE OF CONDUCT.....	15
5	DOCUMENT ADMINISTRATION.....	17
5.1	Document Owner	17
5.2	Document Review	17
5.3	Change history.....	17
5.4	Approval History.....	17

1 INTRODUCTION

Freedom of expression and an open environment to pursue scholarly inquiry and for sharing of information are encouraged, supported, and protected at The New School. These values lie at the core of the university's academic community, and extend to the use of its information resources. However, the use of university information resources, like the use of other university-provided resources and activities, is subject to the requirements of legal and ethical behavior. Thus, acceptable use of a computer, computer system, or network does not extend to whatever is technically possible. The university depends upon a spirit of mutual respect and cooperation to create and maintain an open community of responsible users.

1.1 Objective

This policy establishes the rules for ethical and acceptable use of information resources at The New School. These rules support the free exchange of ideas among members of the New School community and between the New School community and other communities, while recognizing the responsibilities and limitations of such exchange.

1.2 Scope

This policy is an integral part of *The New School Information Security Policy* and applies generally to:

- all students, faculty, staff, contractors, consultants, temporary employees, guests, volunteers, and other members of the university community, including those affiliated with third parties, who access or in any way make use of university information or information systems;
- all university information resources, including those used by the university under license or contract. "Information resources" include information in any form and recorded on any media, and all computer hardware, computer software, and communications networks owned or operated by the university or on the university's behalf; and
- any device, regardless of ownership and including equipment privately owned by faculty, staff, and students (e.g., laptop computers, tablet computers, smart phones, MP3 players, USB storage devices, etc.), but only with respect to the ways in which they connect to or access university information resources and the activities they perform with those resources.

Specifically, the sections of this document apply as follows:

- Section 2, *General Policy on Acceptable Use*, applies to all members of the university community.
- Section 3, *Acceptable Use of Administrative Information Resources*, applies to those members of the university community who use administrative systems, operate administrative client systems, or otherwise access administrative information.
- Section 4, *Privileged User Code of Conduct*, applies to those members of the university community whose jobs require privileged access to university information resources. Typically, such persons are either technical systems administration or programming personnel or administrative employees with some access to the university's databases.

1.3 Compliance

Compliance with this Policy is mandatory for all students, faculty, staff, contractors, consultants, temporary employees, guests, volunteers, and other members of the university community, including those affiliated with third parties, who access or in any way make use of university information or information systems.

1.3.1 Monitoring

The university considers the data processed by and stored on administrative computer systems to be the property of the university. The contents of user accounts are considered to be the property of the authorized user, subject to applicable university copyright and intellectual property policies and applicable federal and state laws.

Individuals should be aware that their use of university information resources, including accessing the Internet or using electronic mail, social media, instant messaging, telephone, or voice mail, are not completely private. While the university does not routinely monitor individual usage of its information resources, the normal operation and maintenance of these resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the provision of service. The university may also specifically monitor the activity and accounts of individual users of university information resources, including individual login sessions, the content of individual communications, and the contents of stored information, with or without notice, when:

- the individual has voluntarily made the information accessible to the public, as by posting to a blog or a Web page;
- it reasonably appears necessary to do so to protect the integrity, security, or functionality of university information resources or to protect the university from liability;
- a written complaint has been received, or there is reasonable cause to believe, that the individual has violated or is violating this policy;
- an account appears to be engaged in unusual or unusually excessive activity; or
- it is otherwise required or permitted by law.

Any such monitoring of communications or stored information, other than what is made accessible by the individual, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the Provost and Chief Academic Officer, the Senior Vice President for Human Resources and Labor Relations, the Senior Vice President for Student Services, or the Senior Vice President for Information Technology, as appropriate, in consultation with the Office of the General Counsel. The university, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications or stored information, to appropriate university personnel or law enforcement agencies and may use those results in appropriate university disciplinary proceedings.

1.3.2 Enforcement

Failure to comply with this policy, whether deliberate or due to careless disregard, will be treated as serious misconduct and may result in actions including (but not limited to) disciplinary action, dismissal, and civil and/or criminal proceedings.

In the case of a written complaint of serious misuse, or evidence indicating that malicious software may be present in certain material on the system, the university reserves the right to temporarily remove material from the system for its review. In some situations, it may also be necessary to restrict or suspend access or account privileges to prevent ongoing misuse while the situation is under investigation.

Alleged infractions of this policy are handled via formal procedures and investigation by the Office of the Provost, Department of Human Resources, or Office of Student Services, as appropriate. Upon determination of misuse, individuals who are found to be in violation of this Policy may be subject to the following:

- restriction or suspension of computer access privileges;
- disciplinary action by their academic division and/or the university up to and including termination;
- referral to law enforcement authorities for criminal prosecution; and
- other legal action, including action to recover civil damages and penalties.

1.4 Exceptions

Exceptions to this policy must be requested using the information security *Procedure for Policy Exception Requests*.

2 GENERAL POLICY ON ACCEPTABLE USE

Users of The New School's information resources must comply with federal and state laws, university rules and policies, and the terms of applicable contracts including software licenses while using university information resources. Examples of applicable laws, rules and policies include:

- the U.S. Electronic Communications Privacy Act, U.S. Computer Fraud and Abuse Act, and Article 156 of the New York Penal Code, which prohibit "hacking," "cracking," and similar activities;
- laws governing libel, privacy, copyright, trademark, obscenity and child pornography;
- the university's Sexual Harassment Policy and Discriminatory Harassment Policy;
- the university's Student Code of Conduct and Employee Code of Conduct; and
- the university's Information Security Policy.

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 jurisdictions and the rules and policies of those other systems and networks.

All users of university information resources are required to have a valid, authorized account, or other form of officially approved access, and may use only those information resources for which they have been specifically authorized. Users are responsible for any activity originating from their accounts which they can reasonably be expected to control. Accounts, passwords, and other access control devices may not, under any circumstances, be used by persons other than those to whom they have been assigned. In cases when unauthorized use of accounts or resources is detected or suspected, the account owner should change the password and report the incident to the Information Technology Helpdesk or the Information Security Office.

2.1 Personal Use of University Information Resources

Authorized users may access The New School's information resources for personal use under certain conditions. Examples of permitted limited personal use include electronic communication with children and dependents, scheduling personal appointments, and use of computers for listening to news and music within reason.

Limited and reasonable personal use is subject to all of the requirements and prohibitions of this policy, as well as the following conditions:

- Personal use of university information resources must not in any way negatively impact the operational needs of the university, or result in any direct cost to the university.
- Personal use of university information resources must not result in commercial gain or private profit, except as allowed under the university Intellectual Property Rights policy. However, in no case may university information resources be used for solicitation or performance of external activity for pay.
- Personal use of university information resources must not state or imply university sponsorship or endorsement.
- Personal use of Internet gaming outside the framework of a course or research project is prohibited.

2.2 Storage of Personal Data on University Computers

Limited personal data may be stored by a user on either his or her computer or network drive with the understanding that:

- Personal data should be stored in a separate and easily identifiable folder so it is easily distinguished from other data.
- No illegal or offensive material may be stored.
- The data stored does not in any way put the system or network at risk.
- The New School is not responsible for the integrity of the data that is stored and makes no guarantee regarding its availability.
- Data is the property of the university and there is no guarantee that the user will be able to retrieve this data upon transfer, resignation, or termination.
- The size and number of files stored is limited and does not place a burden on bandwidth or back-up programs.

2.3 Connection to University Networks

The New School takes measures to protect its computer systems and networks from the effects of malicious software (e.g., computer viruses, worms, Trojan horses, spyware, adware, and malicious mobile code). However, these measures are not foolproof, and computer systems that are not protected can quickly fall prey to malicious software that is distributed through infected web pages (or infected advertisements displayed on legitimate web pages) and unsolicited (“spam”) e-mail messages.

The New School recommends that all non-university computer systems—computer systems owned or operated by students, faculty, staff, contractors, consultants, guests, and volunteers that are used to connect to university computer networks—be protected against malicious software using a reputable malware protection product (commercial, free, or open source). Eligible students, faculty, and staff may obtain a free copy of the corporate malware protection software used by the university through MyNewSchool.

Whatever product is selected, malware protection software should be configured to:

- be active at all times;
- always scan files when they are opened, executed, or downloaded;
- periodically scan the entire system, including memory, hard disks, and USB media; and
- remove malware from the system (e.g., by “disinfecting” files) or quarantine affected files.

Malware protection software should be configured to automatically contact the vendor’s update servers at least once a day to verify that its signature files and scanning engine are up-to-date and install updates if necessary.

2.4 Reporting Security Incidents

Effective security response includes the prompt and appropriate response to breaches in security. It is incumbent on all individuals to report incidents in which they believe the security or privacy of New School information resources has been jeopardized. Individuals are responsible for reporting

security incidents to the Information Technology Helpdesk or the Information Security Office, and for taking action as recommended or directed by those authorities.

2.5 Prohibited and Inappropriate Use

Users of The New School's information resources are prohibited from engaging in any activity that is illegal under local, state, federal, or international law or in violation of university policy. The categories and lists in the sections that follow are not exhaustive, but provide a framework for activities that fall into the category of prohibited and inappropriate use.

2.5.1 Excessive Non-Priority Use of Information Resources

Priority for the use of information resources is given to activities related to the university's academic, research, and public service mission. To conserve resource capacity for all users, individuals should exercise restraint when utilizing computing and network resources. Individual users may be required to halt or curtail non-priority use of information resources, such as recreational activities and non-academic, non-business services.

2.5.2 Unacceptable System and Network Activities

Unacceptable system and network activities include:

- Engaging in or effecting security breaches or malicious use of network communication including, but not limited to
 - Obtaining configuration information about a network or system for which the user does not have administrative responsibility.
 - Engaging in activities intended to hide the user's identity, to purposely increase network traffic, or other activities that purposely endanger or create nuisance traffic for the network or systems attached to the network.
 - Attempting to develop or use any mechanism to alter or avoid charges levied by the university for information resources (e.g., printing).
 - Attempting to intercept network communications for purposes of rerouting packets, forging packets, packet "sniffing," or reading message/file content.
 - Scanning university networks or systems for security vulnerabilities (this includes port scanning).
- Modifying the configuration of the university computing infrastructure in any way including, but not limited to
 - Adding or removing network links, wireless access points, computers, circuit boards, or peripherals (e.g., disks, printers, modems, cameras, etc.).
 - Reconfiguring the university network addressing structure in any way. The university is the sole provider of network services such as Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP), and routing on university networks; any computer or equipment that replicates or disrupts these services will be immediately disconnected.
 - (Re)installing operating systems or changing base configurations on university-owned or -operated systems.
 - Reconfiguring any control switches or parameters.

- Circumventing or attempting to circumvent user authentication and access control mechanisms; accessing or altering data, accounts, or systems that the user is not expressly authorized to access.
- Interfering with or denying service to another user on the campus network or using university facilities or networks to interfere with or deny service to persons outside the university.
- Installing any monitoring device, whether physical or electronic, that attempts to monitor or record the movement or activity of members of the New School community. This includes, but is not limited to the unauthorized installation of webcams for any monitoring purpose within the university, or the use of cell phone cameras for this purpose.

2.5.3 Unauthorized Use of Intellectual Property

Users may not use university information resources to violate the ethical and legal rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations. Violations include, but are not limited to:

- Except as provided by fair use principles, engaging in unauthorized copying, distribution, display, or publishing of copyrighted material including, but not limited to (a) digitization and distribution of photographs from magazines, books, or other copyrighted sources, (b) distribution of copyrighted music or video, and (c) installation of any copyrighted software without an appropriate license.
- Using, displaying, or publishing licensed trademarks, including The New School's trademarks, without license or authorization or using them in a manner inconsistent with terms of authorization. Use of The New School's trademarks and logos must comply with the policies and guidelines published by the Department of Communications and External Affairs.
- Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws.
- Breaching confidentiality agreements or disclosing trade secrets or pre-publication research.
- Using computing facilities and networks to engage in academic dishonesty prohibited by university policy (such as unauthorized sharing of academic work or plagiarism).

2.5.4 Inappropriate or Malicious Use of IT Systems

Inappropriate or malicious use of IT systems includes:

- Using peer-to-peer file sharing programs or file sharing web sites to upload or download protected intellectual property such as copyrighted music or video or illicit copies of licensed software ("warez").
- Intentionally introducing malicious programs into the network or computer systems (e.g., viruses, worms, Trojan horses, spyware, e-mail bombs, etc.).
- Granting any form of information resource access to non-authorized users. This includes, but is not limited to, giving electronic library access to non-authorized persons or any other attempt to give benefit or privilege of the university's information resources to a non-authorized person.

- Attempting to intercept, compromise, or tamper with user passwords. This includes, but is not limited to, copying passwords files, password “cracking,” installing keystroke logging software, intercepting network traffic, or otherwise attempting to discover passwords belonging to other individuals. It also includes taking advantage of another user’s naiveté to gain access to information resources, or preventing someone from using his or her account by changing the password or through other tampering.
- Using a New School information resource to actively engage in displaying, procuring, or transmitting material that is in violation of university codes of conduct, sexual or discriminatory harassment policies or laws, hostile workplace laws, or other illegal activity.

2.5.5 Misuse of E-Mail and Communications Activities

Electronic mail (e-mail) and communications are essential in carrying out the activities of the university and to individual communication among faculty, staff, students, and their correspondents. Some key prohibitions include:

- Sending unsolicited e-mail messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material, except as approved by the Department of Communications and External Affairs.
- Engaging in harassment via e-mail, telephone, paging, texting, or social media, whether through language, frequency, or size of messages.
- Masquerading as someone else by using their e-mail or Internet address or electronic signature, or altering the content of a message from another person with intent to deceive.
- Soliciting e-mail from any other e-mail address, other than that of the poster’s account, with the intent to harass or collect replies.
- Forwarding or otherwise distributing information obtained from another individual that the individual reasonably expects to be kept confidential.
- Creating or forwarding “chain letters” or solicitations for business or quick-profit schemes.
- Using e-mail originating from within The New School’s networks and e-mail systems for commercial purposes or personal gain.
- Sending the same or similar non-business-related messages to large numbers of e-mail recipients or newsgroups.

3 ACCEPTABLE USE OF ADMINISTRATIVE INFORMATION RESOURCES

In addition to the requirements and prohibitions in the previous section, the following requirements and prohibitions apply to the use of administrative information resources.

3.1 Information Ownership and Classification

The New School Information Security Policy establishes security roles and responsibilities for all individuals with access to university information resources. It also establishes classification levels for information that specify the security controls that should be used to protect that information.

- Administrative information must have an assigned Information Owner who is responsible for assigning a classification level to the information, specifying the protection level that should be assigned to the information, and authorizing individuals to access the information.
- Administrative information must be classified as Unrestricted, Restricted, or Confidential by the Information Owner. The classification level should be communicated to all users of the information (e.g., by labeling or other method).
- Administrative information, wherever it resides, is the property of The New School and must be handled in accordance with its classification level.
- Access to administrative information is granted on a need-to-know basis. Attempts to access information for which the user does not have a job-related need to know are strictly prohibited.
- Administrative information may not be published, given away, sold, or disclosed to unauthorized persons without proper authorization.
- Use of administrative information for personal or non-university commercial purposes is strictly prohibited.
- Administrative information must not be represented as official university information for any purpose unless designated as official by appropriate management.

3.2 Maintaining the Security of Classified Information

Administrative information must be handled in accordance with its classification level. Specific requirements for handling information of different classifications can be found in the information security standard document entitled *General Controls for Handling Sensitive Information*. In addition:

- Users granted access to Confidential or Restricted administrative information are responsible for safeguarding that information from disclosure to unauthorized persons. This responsibility applies to all locations and forms of the information—computer workstation files, USB storage devices, CDs and DVDs, print-outs, faxes, etc.
- Confidential information must not be sent via electronic mail, even from one New School user to another, unless that information is encrypted. In general, the New School Secure File Transfer solution provided by the Office of Information Technology should be used for this purpose.

- Requests from law enforcement agencies (including search warrants and subpoenas) for access to administrative or student information must be referred to the Office of the General Counsel.
- Federal and state statutes and regulations govern certain university administrative information. All Information Owners and the managers and administrators of systems in which regulated data is created, maintained, or stored must be aware of the provisions and requirements of all applicable laws and regulations. These laws and regulations include, but are not limited to:
 - The Family Educational Rights and Privacy Act (FERPA) governs what information about students may be considered public and what information must be protected, and students' rights with respect to that information.
 - The Gramm-Leach-Bliley Act of 1999 (GLBA) requires organizations that provide financial services (e.g., student loans) to protect the security and confidentiality of individuals' personally identifiable financial information.
 - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects the privacy of health information created, transmitted, or maintained by health care providers and other institutions by electronic means. The services provided by Student Health and Support Services do not qualify The New School as a "covered entity" under HIPAA; however, information collected in the provision of these services is subject to protection under FERPA.
 - New York State General Business Law 399-dd governs the protection of faculty, staff, and student Social Security numbers.
 - New York State General Business Law 899-aa governs unauthorized access (disclosure) to certain elements of individuals' personally identifiable information and the notification process that The New School must follow in the event of such access.
- When no longer needed, administrative information must be disposed or destroyed using secure methods that ensure the information is rendered irrecoverable; these methods are specified in the information security standard document entitled ***General Controls for Handling Sensitive Information***. Likewise, decommissioned information systems equipment must be sanitized or destroyed to remove any administrative information prior to disposal.

3.3 Use of Administrative Computers

Because of the nature of the information they process, administrative computers cannot be as open and accessible as the computers used in student lab facilities, classrooms, and for research purposes. Users of administrative computers may not:

- Install or use any file sharing program or any other program that makes the content or the configuration of the system visible or accessible to external entities.
- Install or use plug-ins or interfaces that change the security configuration of web browsers or systems, or that allow the monitoring of any system settings by external entities.
- Install or use any program that establishes a permanent connection between the system and an external server.

- Install any program that offers services from the system to others (e.g., web servers, file servers, print servers, etc.) without prior approval from the Office of Information Technology.
- Install any program that does not directly support the administrative function of the university, other than those programs that have been approved by the Office of Information Technology.
- Install or enable any remote access/remote management software or functionality on the system, other than those programs/functions that have been approved by the Office of Information Technology.

Users of administrative computers should:

- Choose difficult-to-guess passwords—at least eight characters in length, containing a mixture of uppercase, lowercase, numbers, and punctuation—and change them frequently (e.g., every three months).
- Use a password-protected screen saver to prevent unauthorized access to the system when their computer is unattended for short periods.
- Cooperate with on-screen prompts to permit the installation of operating system and software security patches; some of these prompts may require the system to be restarted.
- Log off of the system at the end of the workday.

4 PRIVILEGED USER CODE OF CONDUCT

Certain individuals are given privileged access to computer systems because their job responsibilities require such access. Typically, such individuals are either technical system administration or programming personnel, or are administrative employees with some access to the university's main databases. These privileged users have the ability, through user names, passwords, and other mechanisms, to bypass the usual security features of the system in order to perform administrative and maintenance operations.

This code of conduct applies to all persons given privileged access to university computer systems, networks, administrative applications, or administrative databases. It also applies to the persons who authorize such access.

Privileged users are bound by the following conditions in addition to the requirements and prohibitions set forth in Section 2, *General Policy on Acceptable Use*, and Section 3, *Acceptable Use of Administrative Information Resources*. Privileged users may not:

- Use their privileged access to “browse” through information (files, electronic mail messages, etc.) owned by other system users. Exceptions to this rule are when such browsing is a specific part of their job description (e.g., a corporate auditor); is required during file system repair, management, or restoration; is necessary to investigate suspicious or system-impairing behavior, or possible violations of university policy; or is specifically requested by, or has the approval of, the person who authorized their privileged access. (See also Section 1.3.1, *Monitoring*.)
- Use their privileged access to engage in so-called “administrative voyeurism” (that is, any form of personal information viewing not directly related to an employee’s task. This includes but is not limited to seeking personal, financial, or medical information on students, employees, donors, or alumni).
- Use their privileged access to change any information about themselves.
- Disclose, to any unauthorized person, information observed while operating with privileged access.
- Copy any information for any purpose other than those authorized under their defined job responsibilities or pursuant to an authorized investigation or review.
- Do any special favors for any user, member of management, friend, or any other person regarding access to New School computers. Such a favor would be anything that circumvents prevailing security protections or standards or in any way unfairly advantages one user over others.
- Disclose to any unauthorized person the information required to gain privileged access, or to engage in careless practices that would reveal that information to unauthorized persons.
- Attempt to gain or use privileged access outside of assigned responsibility (e.g., on other machines) or beyond the time when such access is no longer required in assigned job functions.
- Change or develop any computer software in a way that would disclose information to persons not authorized to have it, or make it possible to retain any special access privilege once that authorized privilege has been terminated by management.

5 DOCUMENT ADMINISTRATION

5.1 Document Owner

This document is owned by the Information Security Office, which is responsible for its content and maintenance.

5.2 Document Review

This document is subject to review on an annual (or more frequent, if necessary) basis to validate that its content remains relevant and up-to-date. Significant or material changes to this document must be reviewed and approved by the Information Security Steering Committee.

5.3 Change history

Version	Description	Author	Date
1.0	Initial publication	D. Curry	18 Nov 2011

5.4 Approval History

Version	Name	Title	Date
1.0	Information Security Steering Committee Marla Appelbaum Jacob Campbell Alex Carnes Tara Creagh David Curry Robert Lutomski Robin Lynn Charis Ng Natalie Pressey Donna Puchalski Shelley Reed Elizabeth Ross Paul Shosho Keila Tennent	Sr. Director, Design & Construction Asst. Director, Advancement Information Services Asst. University Registrar Sr. Benefits Specialist, Human Resources Director, Information Security Director, Student Housing Assoc. Director, Online Media Assoc. Director, Institutional Research Asst. Vice President & Comptroller AVP, Payroll & Tax Compliance Sr. Vice President, Information Technology Vice Provost Director, Financial Systems & Analysis Assoc. General Counsel	18 Nov 2011