William Paterson University

Information Technology Policies

Introduction

The following series of policies govern the use of William Paterson University information technology services and resources by all faculty, staff, students and other authorized users. These services and resources are provided by the University to support its mission of teaching, research and public service as carried out by the various members of the University community. Recognizing the ubiquitous and changing nature of information technology services and resources, the Policies strive to provide the fundamental principles necessary to balance and understand divergent interests and needs of the University community.

The Policies are organized into four main sections, each with several sub-sections. The main sections are: Appropriate Use, Electronic Communication, University-Produced Electronic Data and Files and Network Infrastructure Security.

Section 1: Appropriate Use Policy

Three principles provide the foundation upon which the University's Appropriate Use Policy is based. These are:

- University information technology resources and services are owned by the University and provided to authorized users (faculty, staff and students) for the purpose of assisting them in carrying out University-related activities. As a community service, the University also provides Internet access to registered Guests from workstations in the Cheng Library. Guest Accounts for members of the public and for visiting lecturers, etc are created by appropriate University staff on a short-term basis. Individuals with Guest Accounts are also considered to be authorized users.

- Users of University information technology services and are bound by all local, state and federal laws pertaining to the use and dissemination of information and data created, compiled or accessed by the University's information technology resources and services.

- As members of the University community, faculty, staff, students and other authorized users of these resources will act responsibly and ethically in their use of information technology resources and services.

Subsection 1.1: Privacy

1.1.1 All authorized users of William Paterson University's information technology resources and services may expect that their communications and files are generally private and confidential. Other than in the following exceptional instances, the University will not randomly or routinely monitor any form of communication or access user files. The University may monitor and/or read user communications and files only under these conditions:

1.1.1a When required to do so by judicial actions such as search warrants

1.1.1b When investigating possible violations of University policy or law
1.1.1c When individuals are no longer authorized users and the conduct of University business necessitates access to such information

1.1.2 In such extraordinary circumstances, University officials will observe the following procedures:

1.1.2a Requests to view user electronic mail or files of employees or authorized users will be submitted to the President, Provost and the Vice President for Administration and Finance for approval. At least two of these three administrators must approve the request.
1.1.2b Requests to view user electronic mail or files of students will also be reviewed and approved by the Vice President of Student Development.
1.1.2c All other Vice Presidents will be notified of such requests.
1.1.2d Unless notification would compromise the investigation of either illegal activity or violations of University policy, the person(s) whose files are to be monitored will be notified as soon as possible. Records of the monitoring activity will be kept.
1.1.2e Any information discovered during this investigation that does not relate to the specific alleged violation of law or policy will be immediately destroyed, except as may be otherwise required by law or University policy. All information retained will be kept secure.
1.1.2f University officials will annually report to the Faculty Senate on the number and general reasons for all monitoring incidents.

Subsection 1.2: Responsible Use

Users of University information technology resources and services agree to act responsibly with respect to their fellow community members and these resources. Such responsible use includes, but is not limited to:

1.2.1 Restricting use of University resources to the level necessary to conduct University business
1.2.2 Acting prudently so as not to diminish the availability of information technology resources for other members of the University community
1.2.3 Notifying appropriate System administrators of any breaches in security that would compromise either the network or the privacy of others

Subsection 1.3: Access to Information Technology Resources and Services

Access to the University's information technology resources is a privilege granted to faculty, staff, students and other authorized users for the purpose of teaching, learning and related University business. In order to protect and maximize this access to computing facilities, the following policies apply:

1.3.1 User account authorization is required for access to the University network, which includes connecting to the Internet and to the University's information and application systems' resources.

1.3.2 All faculty, students and staff will be assigned individual user accounts and each will create his/her own confidential password for authentication purposes.

1.3.3 Under certain circumstances, such as a courtesy to community users of the Library and for guest lecturers and scholars, Guest Account Access may be authorized by Information Technology administrators or, in the case of the Library, by designated Library staff [see Appendix A for complete policy on Library Guest Account Access].

1.3.4 All computers and devices used to access the University's network must conform to the University's security standards [See Appendix B for a complete description of these standards]. Unauthorized connectivity or use of any computer or device not conforming to these security standards will be denied access by the University's Network administrators.

Subsection 1.4: IT System Administrator Responsibilities and Privileges

As an efficient and effective method for administering the University's information technology resources, the IT department provides a standard computer configuration managed by its System Management staff. System-wide privileges for installing hardware and software and for trouble-shooting problems are provided to authorized IT administrators. In certain circumstances and according to the Systems Administrator Access Agreement [see Appendix C for this Agreement], the following exceptions are made:

1.4.1 As necessary and as governed by the Agreement outlined in Appendix C, certain non-administrative faculty and staff may obtain System Administrator Access to University computers assigned to them for the purpose of installing software or hardware necessary required for teaching or other University business

1.4.4 No level of System Administrator Access privileges may be used to gain unauthorized access to any user accounts or to block authorized access to University-assigned computers or devices.

Subsection 1.5: Legal Requirements Affecting Information Resources and Services

All users of University-provided information technology services and resources are obligated to comply with all federal, state and local laws and regulations. These laws and regulations include, but are not limited to the following:

1.5.1 Copyright

1.5.1a Print, digital materials, software and other non-print materials, including web pages, are equally subject to copyright laws and policies. The University prohibits faculty, staff, students or other authorized users from using University-owned technology resources, equipment or services to access, use, copy or otherwise reproduce, or make available to others any copyright-protected digital materials or software except as permitted under copyright law (especially with respect to “fair use” interpretations) or specific vendor licenses.

1.5.1b Copyright policies and practices to which members of the University must adhere are described at the following links on the University Library’s web site as follows:
Introduction: http://www.wpunj.edu/library/copyright_main.shtml
Copyright Policy: http://www.wpunj.edu/library/copyright_policy.shtml
Fair Use Guidelines: http://www.wpunj.edu/library/copyright_fair.shtml

1.5.1c The University is obligated to comply with the Digital Millennium Copyright Act of 1998 (http://www.copyright.gov/legislation/dmca.pdf). Users of software programs such KaZaa, BitTorrent and LimeWire to listen to or view digital files must assure that they do not violate copyright restrictions by sharing copyright protected materials over the University network.

1.5.1d The University respects the copyright protections provided by federal law to all copyright holders, including digital materials and software.

1.5.1e Software applications provided by the University for use by its faculty, staff, students and other authorized users may be used only on computing equipment and in the manner authorized by the relevant vendor licenses. The University regards violations of these policies as serious offenses and any such violation is without its consent and is subject to disciplinary action. Repeated violations will result in loss of computing privileges, among other sanctions. (Adapted from the University of Virginia, http://www.itc.virginia/edu/policy/copyright.html)

1.5.1f Copyright infringement complaints pertaining to the Digital Millennium Copyright Act may be filed by sending an e-mail to an account established for this purpose.

1.5.2 USA Patriot Act

1.5.2a All users of the University’s information technology services and resources are obligated by law to comply with the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" (USA PATRIOT) Act. The act, as relevant for IT policy purposes, expands law enforcement's surveillance and investigative powers with respect to library records and electronic communication. The USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. 109-177, 120 Stat.192 (Mar. 9, 2006), *is available at* http://thomas.loc.gov/bss/d109/d109laws.html

1.5.3 HIPAA

1.5.3a The University is obligated by law to comply with the Health Insurance Portability and Accountability Act of 1996. The act, as relevant for IT policy purposes, requires institutions to meet specific standards with respect to the privacy, transmission and electronic security of health records, such as are maintained by our Health and Wellness Center. The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (Aug. 21, 1996), *is available at* http://thomas.loc.gov/bss/d104/d104laws.html

1.5.4 FERPA

1.5.4a The University is obligated by law to comply with the Family Educational Rights and Privacy Act. This act, as relevant for IT policy purposes, describes how students and others may obtain access to University student records, including those stored electronically. The University's FERPA policy is published in the Student Handbook. The Family Educational Rights and Privacy Act of 1974, Pub. L. 93-380, 88 Stat. 484, (Aug. 21, 1974), *is available at* http://uscode.house.gov/download/pls/20C31.txt

1.5.5 GLB

1.5.5a The University is obligated by law to comply with the Gramm-Leach-Bliley Act (also known as the Financial Services Modernization Act). This act, as relevant for IT policy purposes, requires institutions to protect student financial information obtained electronically or on paper in the course of doing business with that student.

Student financial information is that information that William Paterson University has obtained from a customer in the process of offering a financial product or service, or such information provided to the University by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent(s) when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format. *(This paragraph adapted from Kansas State University http://www.k-state.edu/policies/ppm/3415.html#intro)* The Gramm-Leach-Bliley Act of 1999, Pub. L. 106-102, 113 Stat. 1338 (Nov. 12, 1999), *available at* http://thomas.loc.gov/bss/d106/d106laws.html

1.5.6 New Jersey State Office of Information Technology (OIT)

1.5.6a As a public institution, the University is required by State law to comply with the policies and standards of the State OIT as applicable to institutions of higher education. http://www.state.nj.us/it/ps/

Section 2: Electronic Communication Policies

E-communications include all of the various electronic communication methods available to members of the University community. These are e-mail, the University's web site and the University's web portal, WPConnect.

Subsection 2.1: E-mail

2.1.1 Upon appointment/admission to the University, all faculty, staff and students are assigned University e-mail accounts and provided with instruction in their use.

2.1.2 These accounts are provided in order to assure timely, efficient and verifiable communication between individuals and departments for instructional and administrative purposes. Therefore, the University will use e-mail as an official means of communication to all faculty, staff and students. All members of the community are expected to monitor and manage their University e-mail accounts on a regular basis and each person will be held responsible for information sent to his/her University e-mail account.

2.1.3 This practice is particularly important for students since important information pertaining to admission, financial aid, registration, billing, class assignments, etc. may be sent *only* via e-mail.

2.1.4 Personal use of the University-assigned e-mail account is expected to be incidental and occasional. It may not interfere with the work of an employee nor consume resources that are needed for University business.

2.1.5 While the University does not monitor or censor e-mail, all users must understand that e-mail can be reviewed as required by law or violation of University policy as outlined in Section 1.1 (Privacy) of the University's Appropriate Use Policy.

Subsection 2.2: University Web Sites

2.2.1 The University's home page and departmental web pages featured on the main web site, WPUNJ.EDU, are presentations of official University information and therefore constitute another means of official University communication to community members.

2.2.2 Official University data published on the University's website must be maintained by the office responsible for that data and all other web references to that data should be provided as links to the original source. Offices responsible for data published on the University's website must review that data for accuracy and currency on a regular basis.

2.2.3 The University web site is used for making timely announcements of University news, for communicating emergency information and for providing information about events and activities to both internal and external audiences.

2.2.4 The University's web portal, WPConnect, serves as a vehicle for internal communications only to authorized members of the University community. It is another method for the delivery of official University communication and members of the community are expected to monitor it regularly.

2.2.5 Some sections, or tabs, of WPConnect, such as Student Life, are provided for ease of communication to student groups and thus contain information that is not official University information.

2.2.6 The web portal also provides authorized access to self-service web applications for administrative functions.

Subsection 2.3: Personal Web Pages

2.3.1 The University permits members of the community to host personal web pages on University servers as a courtesy and to facilitate their educational and professional goals.

2.3.2 University-hosted personal web pages may not be used for commercial purposes and users are prohibited from accepting remuneration of any kind derived from information published on these personal web pages. Commercial advertisements are prohibited, although links to commercial sites are permitted.

2.3.3 Users who publish personal web pages on University servers agree to take full responsibility for the content of their materials and agree to comply with all applicable University policies and local, state and federal laws.

Section 3: University-produced Electronic Data and Files

Subsection 3.1: Protection of Personal Non-public Information about University Faculty, Staff, and Students

3.1.1 The University protects confidential information about its faculty, staff and students and acquires and retains only the personal non-public information necessary for carrying out its academic, health, employment and business obligations.

3.1.2 For these purposes, personal non-public information is considered to be information or data that could be used to access other confidential information about a person, thus making a person vulnerable to identity theft. Excluded from this category of data are general, directory-type information. Also excluded is any information which is defined as public record by laws such as the Open Public Records Act (OPRA) for staff and FERPA for students.

3.1.3 In accordance with the NJ Statute 18A:3-28 (2006), personally identifying non-public information will not be publicly accessible or displayed.

3.1.4 Information about a person or about a person's computer use may also be obtained as a result of the University's use of "cookies" and computer system log files. This information is captured when a person interacts with the University's website or uses a University-owned computer. This information is used by the University to facilitate user access to applications, such as WPConnect, and by University staff to evaluate its web services.

3.1.5 Access to University-retained, personal non-public information about University faculty, staff and students may be granted by the steward of that information based upon the following factors: relevant laws and contractual obligations, the requester's need to know, the sensitivity of the information and the risk of damage to, or loss by, the University.

3.1.6 In the event of a computer security breach, all persons whose personal information might have been acquired in an unauthorized manner will be notified in a timely manner. A University computer security system breach is defined as unauthorized access (including copying or reading) to otherwise secure data.

Subsection 3.2: Retention and Storage of Personal Non-Public Information

3.2.1 University offices will retain only the personal non-public information to carry out its educational mission or as required by law.

Appendix A: Cheng Library Guest Account Authorization

In an effort to safeguard the security of its computer network, William Paterson University requires each user to sign-on with his/her personal, University-assigned username and password. Because the Cheng Library has a tradition of offering access to Library resources, both print and electronic, to non-University users, Guest Accounts are provided as a courtesy to community users, visiting scholars and University alumni. Guest Accounts are intended only for use of the of the Library's electronic resources or to gain access to the Internet. In most cases, the access will expire within three days, although exceptions to this general rule may be made for visiting scholars at the discretion of the Library Director. Guest Account access for alumni generally will expire within 30 days. Users of Guest Accounts shall observe the requirements set forth in the University's Policy on Responsible Computing accessible at http://ww2.wpunj.edu/itservices/policies/wpu_aup.htm. Guest Account Users will acknowledge their acceptance of this policy and the Guest Account Access Policy by signing a form provided at the time the guest account is created.

University faculty, staff and students have priority in the use of computing facilities. Individuals with Guest Account privileges may use these facilities on an as-available basis and must yield to priority users when requested to do so. Guest Account privileges do not include University email accounts, access to network file storage or access to, or use of, the University's and Library's wireless laptops or network. It also does not include access to Library databases from locations beyond the Cheng Library.

Library staff retain the right to refuse the Guest Account privilege to alumni and community users who do not provide appropriate identification (see below). The University is not responsible for documents created or activities pursued by users with Guest Account privileges.

Acceptable forms of identification

Alumni requesting Guest Accounts may provide a valid Alumni Card as acceptable identification but they must also provide proof of current address, such as valid driver's licenses or current mail from a municipality (such as a tax bill), telephone, utility or credit card company.

All other requestors must provide both photo identification and documentation of their current address. Acceptable forms of photo identification include valid drivers' licenses, government-issued photo identification cards, passports or other, third-party issued photo IDs. Third-party issued identifications, such as those from an employer, a college, university or school, or a membership organization must contain a laminated photo and embossed name of the issuing agency. Acceptable forms of current address documentation include valid driver's licenses or current mail from a municipality (such as a tax bill), telephone, utility or credit card company.

Appendix B: William Paterson University Information Technology Security Standards

While the Information Technology units provide hardware and software safeguards, the overall security of the University's technology resources and information is a shared responsibility. The advantages of the Internet and ease of access to information and services are continually challenged by the risks of on open environment subject to abuses and intentional and unintentional misuse. In order to maximize the delivery of information and services and minimize risks, the University community must actively participate in security measures and guidelines and always be diligent in the use of information resources.

Secure Access:

User Accounts: User account authentication is required to access University technology resources. Individual accounts provide accountability for accessing University information resources and provide access to personal information. User account information (usernames and passwords) should never be shared nor should users ever access someone else's account. Failure to retain the confidentiality of one's user account may result in providing unauthorized access to the system and being held responsible for the actions of others.

Passwords: The purpose of passwords is to protect user accounts. Since the University uses a standard for user accounts (last name, first initial) the diligent creation and protection of passwords is a fundamental security responsibility of all users. Passwords should be a string of not less than 6 characters and include numbers and symbols. Recommended methods for protecting passwords include: a) use of a phrase instead of a single word; b) use uncommon names or words; c) memorize passwords rather than listing them.

As a best security practice, the University will sometimes require all users to create new passwords.

Identity Protection:

Federal and State law including FERPA, HIPPA, etc. provide strict guidelines to protect personal information. The University is also required by state law to limit and protect the use of social security numbers.

> *NJ 18A:3-28 (Effective January 26, 2006) Display, certain, of student's social security numbers prohibited.*
>
> *No public or independent institution of higher education in the state shall display any students social security number to identify that student for posting or public listing of grades, on class rosters or other lists provided to the teachers, on student identification cards, in student directories or similar listings, unless otherwise required in accordance with applicable state or federal law.*

In addition to complying with the State legislation, the use of social security numbers as the primary identification key on files and records within offices and departments must be replaced with use of student and employee "855" identification numbers.

Remote access:

The University's home web page and associated links are intended for general public access via the Internet. All other remote access to University databases and proprietary information are restricted to authorized use and subject to additional security. This includes following:

> * Data encryption is required for all web pages that transmit personal records and information.
> * Remote access to University Enterprise Systems must be on a secure connection such as Virtual Private Network (VPN) which includes authentication and encryption.
> * A secure connection is required on any remote connection behind the University's firewall.
> * University laptops and computers, and personal computers used off campus must not download and store files that include social security numbers or other legally protected personal information.

Security Tools:

The Information Technology units will utilize security tools to monitor and protect the University from unauthorized access and from threats that may jeopardize the network or computing environment. These tools and associated systems management will block or remove security risks from the University's network and computing environment.

> * Firewall protection is deployed to block unauthorized access to the network, servers and databases. All University databases and computer records, including departmental or individual user files, that contain legally protected personal information must be firewall protected.
> * A suite of software tools are deployed to minimize the risks of computer viruses and related threats. All University computers will have updates to definitions applied automatically, or made available for individual updates.
> * All personal computers connecting to the University's network resources may be scanned for having appropriate levels of security. Access can be denied in cases where any computer or technology device presents a risk to the network or computing environment.
> * Network and server performance will be monitored. Actions will be taken to minimize risks such as illegal file sharing or any action that may jeopardize the University's information technology resources.

Appendix C: System Administration Access Agreement

University owned computers are provided to faculty and staff with a standard configuration. The local operating system and software installation are managed by Information Technology units responsible for supporting these computers and ensuring the integrity of these systems including licensing, security updates and software release levels.

It is anticipated that individuals and departments will have a need for additional software tools or applications that is not a part of the standard configuration. In these cases it is strongly recommended that a request for additional software be made to Information Technology to assist in the installation. The software request procedure: http://ww2.wpunj.edu/ITSERVICES/policies/request1a.htm will prompt for information that will help maintain the integrity of the local computer and develop the most effective installation method. Installation of additional software can be done remotely by Information Technology, or by a Support Specialist on the local machine, or by the individual user, whichever best meets the need.

In some cases faculty or staff members may feel they need to have administrative-level access to their computer. This level of access is discouraged because it not only permits the installation of software and hardware, but enables changes to the standard configuration. Changes to the standard configuration can increase the risks of spy-ware and other security issues. Individuals must make a formal request for administrative-level access and agree to the following terms and conditions.

1. Future University system upgrades of software and hardware may require users to reinstall locally installed software or hardware.

2. If performance or system problem issues arise, the Information Technology units will only be responsible for reinstalling the University's standard configuration. User may need to reinstall local software or hardware and restore associated data stored locally.

3. The Information Technology administrative-level access to the machine as delivered in the standard configuration must remain in tact. Any blocking of university access to the machine will result loss of network access.

4. Security updates will automatically be delivered to all university computers. Security updates are the responsibility of the user if the standard image is not being used and preventing automatic security updates. Any computer not meeting University level security standards will result in loss of network access.

5. Updated versions of standard configuration software will be delivered automatically. Administrative-access level users can make arrangements for updated versions of software to be done by the IT units, or locally, but any performance issue will be referred back for re-install of the University's standard configuration.

6. Per the University's Guidelines for Responsible Computing, Information Technology reserves the right to disconnect any device from the campus network if that device is causing undue network traffic, or is suspected of having a security breach. Per this agreement, if a disconnect is required by Information technology, the Administrative User will be responsible for taking any corrective action before the machine will be reconnected to the campus network.

A request for Administrative-Level Access is available at:
http://www.wpunj.edu/itservices/policies/LocaL_Admin_Privileges_requests_Policy.htm