William Paterson University Policy
University Policy

SUBJECT:	University Policy		**TITLE:**	Technology Services and Resources			
CATEGORY: Check One	**Board of Trustees** ☐	**University** ☒		**Functional** ☐		**School/Unit** ☐	
Responsible Executive:	President and Cabinet Members			**Responsible Office:**	Information Technology		
CODING:	00-01-	**ADOPTED:**			**AMENDED:**		

LAST REVIEWED: xx/xx/xx

I. PURPOSE

This Policy governs the use of William Paterson University technology services and resources. 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 Policy strives to provide the fundamental principles necessary to balance and understand divergent interests and needs of the University community.

II. ACCOUNTABILITY

While the Information Technology Department provides 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 technical resources

III. APPLICABILITY

All faculty, staff, students and other authorized users.

1V. BACKGROUND

University technology resources and services are owned or operated by, or on the behalf of, 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 and Intranet access to registered Guests. Guest Accounts for members of the public and for visiting lecturers, consultants, vendors, etc. are created by appropriate University staff on a short-term or long-term basis. Individuals with Guest Accounts are also considered to be authorized users.

Members of the University community should have no expectations of privacy with regard to their use of the University's technology services and resources, including, but not limited to, the contents of email, attachments to email and World Wide Web browsing. The University reserves the right to archive, monitor, review and/or disclose electronic messages and information.

V. REFERENCE(S)

Users of University technology 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 technology resources and services.

VI. POLICY

A. Requirements: 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 technology resources and services.

a. Access to the University's 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 is mandatory:

i. 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. Multi-Factor authentication must be used when required.

ii. All faculty, students and staff will be assigned individual user accounts and each will create his/her own confidential password, in compliance with the University's complexity standard, for authentication purposes. The assigned account username and display name will be the legal last name and the first letter of the legal or affirmed/preferred first name. If the last name and first initial are not unique then a number will be added to the username. In addition, all account holders must subscribe to the secondary Multi-Factor secondary logon process if implemented for the resources they use.

iii. Under certain circumstances, as a courtesy to guest lectures, scholars, conference or program attendees, vendors, etc. guest account access may be authorized by Information Technology or designated Cheng Library personal. In addition, WiFi guest access may be granted by authorized University account holders.

iv. All computers and devices used to access the University's network must conform to the University's security standards.

b. System Administrator Responsibilities and Privileges are an efficient and effective method for administering the University's technology resources. Information Technology (IT) provides a standard non-privileged computer configuration, managed by User Services in labs and University PC's provided to employees and students. System-wide privileges for installing hardware and software and for trouble-shooting problems are provided to authorized IT personnel. Faculty and staff may request IT grant System Administrator Access to University computers assigned to them for the purpose of installing software or hardware necessary for teaching or other University business. IT, based on recommendations from Department Chairs, Department Directors, or University Administration, at its sole discretion, may grant on a temporary or permanent bias, System Administrator Responsibilities and Privileges 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.

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

i. Copyright: 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 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. Users of software programs 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. Copyright infringement complaints pertaining to the Digital Millennium Copyright Act may be filed by sending an e-mail to copyright@wpunj.edu.

ii. USA Patriot Act: All users of the University's 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 technology services and resources policy purposes, expands law enforcement's surveillance and investigative powers with respect to library records and electronic communication.

iii. HIPAA: The University is obligated by law to comply with the Health Insurance Portability and Accountability Act of 1996. The act, as relevant for technology services and services 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.

iv. FERPA: The University is obligated by law to comply with the Family Educational Rights and Privacy Act. This act, as relevant for technology services and resources 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 and the University Policies Web Site.

v. GLB: 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 technology services and resources 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.

vi. NJ-OIT: As a public institution, the University is required by New Jersey State law to comply with the policies and standards of the New Jersey State Office of Information Technology (OIT) as applicable to institutions of higher education.

d. Electronic Communication include all of the various methods available to members (e-mail, web site and portal) of the University community are subject to the following:

i. Upon employment by or admission to the University, all employees and students are assigned University e-mail accounts. 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 from their University e-mail account. This practice is particularly important for students since information pertaining to admission, financial aid, registration, billing, class assignments, etc. may be sent only via e-mail.

ii. 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. 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.

iii. 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. 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.

iv. 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. Some sections, or tabs, of WPconnect, are provided for ease of communication to student groups and the campus community thus may contain information that is not official University information.

e. 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 educations mission, employment, and business obligations or as required by law. Access to sensitive data is restricted to those who have a need to know as defined by job duties. Anyone who receives and maintains sensitive data has a responsibility to maintain and safeguard the data.

i. 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.

ii. 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 technical services.

iii. 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.

f. Users must not engage in activity outside the limits of access that have been authorized for them. This includes but is not limited to:

i. Performing an act that negatively impacts the operation of computers, peripherals or networks, or that impedes the ability of someone else to do his/her work. Examples include but are not limited to:

1. Tampering with any transmission medium or hardware device, or connecting any unauthorized device (such as a router, switch, hub, wireless access point, etc.) or computer to the University network.
2. Propagating a software virus or worm.
3. Damaging or destroying data owned by the University or someone else.
4. Modifying any disk or software directory.
5. Performing an act that places an unnecessary load on a shared computer or the University network.
6. Illegal file sharing

ii. Attempting to circumvent protection schemes for access to data or systems, or otherwise uncover security loopholes.

iii. Gaining or granting unauthorized access to computers, devices, software or data. This includes, but is not limited to:

1. Admitting someone into a locked facility, or unlocking any facility that is normally locked, without permission.
2. Giving account passwords to individuals who are not the owners of such accounts.
3. Obtain passwords to or use of accounts other than one's own.
4. Permitting the use of any account, including one's own account, in a way that allows unauthorized access to resources.

iv. Using the University's facilities to send or broadcast unauthorized content. Examples include but are not limited to:

1. Advertising campaigns for personal financial gain or political purposes.
2. Pranks and chain messages.
3. Announcements not approved for dissemination.
4. Transmission of any graphic image, sound or text that is sexual in nature.
5. Use of offensive or discriminatory language.
6. Harass, threaten, or otherwise invade the privacy of others.
7. Confidential or classified information.

v. Using University facilities for personal gain, or for the benefit of an organization other than the University.

B. Responsibilities:

Departments are required to make sure all employees are aware of this Technology Services and Resources policy and formulate business processes that are consistent with the policy.

C. Enforcement:

Use of any computer or device not conforming to security standards will be denied access by Information Technology.

Failure to adhere to the Technology Services and Resources policy may constitute cause for disciplinary action.

VIII PROCEDURE(S)

If a data security incident is suspected, the Information Technology Helpdesk must be contacted immediately. The Information Technology Helpdesk will immediately inform the Chief Information Officer (CIO), Director of Users Services, Director of Enterprise Network and System Services, and Information Security Architect. Employees may not make changes to the affected system in order to preserve valuable forensic evidence

IX. EXHIBIT(S) (optional)

(This section includes forms, illustrations, bibliographies and reference information.)

By Direction of the President and Cabinet:

Date

_____

(Title of Executive or Vice President(s) whose area of responsibility the policy covers.)