# Information Technology Policies and Procedures

## Acceptable Use Policy

### *Overview*

This policy is intended to protect the University's faculty, employees, Students and employees as well as the University from the consequences of illegal or damaging actions by individuals using the University Information Technology Network.

The University Information Technology Network includes: Internet/Intranet/Extranet-related systems, including but not limited to computer/Networking equipment, Software, Operating Systems, storage media, Network accounts providing electronic mail, Instant Messaging, student information system, WWW browsing, and FTP, which are the property of the University. They are to be used for University business purposes and to serve the interests of the University, and as well as all Authorized Users. Effective computer Security is a team effort requiring the participation and support of every University faculty member, employee, student and Authorized User who deals with information and/or information systems. It is the responsibility of every computer user to know the University Information Technology Policies and Procedures, and to comply with the University Information Technology Policies and Procedures.

### *Purpose*

This policy describes the Authorized Use of the University Information Technology Network and protects the University and Authorized Users. Unauthorized uses expose the University to many risks including legal liability, Virus attacks, and the compromise of Network systems, Services, and information.

### *Scope*

This policy applies to all persons with a Park University-owned, third party-owned, or personally-owned computing device that is connected to the University Information Technology Network.

### *Policy*

**General Use and Ownership**

- Data created by Authorized Users that is on the University Information Technology Network is the property of the University. There is no guarantee that information stored on the University Information Technology Network device will be confidential.

- Authorized Use includes reasonable personal use of the University Information Technology Network by Authorized Users. University departments are responsible for creating guidelines concerning personal use of the University Information Technology Network. In the absence of such guidelines, employees should consult their supervisor, manager, or the Information Security Guidelines; Students should consult the Student Assistance Center.
- Any information that an Authorized User considers to be sensitive or vulnerable should be encrypted. For guidelines on information classification, see Information Security's Information Sensitivity Policy. For guidelines on encrypting Email and documents, consult Information Security's Awareness Initiative.
- Authorized University employees may monitor the University Information Technology Network traffic at any time, in accordance with the Information Security Audit Policy.
- The University reserves the right to audit Networks and systems on a periodic basis to ensure compliance with the University Information Technology Policies and Procedures.

**Security and Proprietary Information**

- Authorized Users are required to classify the user interface for information contained on the University Information Technology Network as "confidential" or "not confidential," as defined by University Confidentiality Guidelines. Confidential information includes, but is not limited to: University private data, specifications, student information, and research data. Employees are required to take all necessary steps to prevent unauthorized access to this Sensitive Information.
- Authorized Users are responsible for the Security of their passwords and accounts and must keep passwords confidential and are not permitted to share accounts.
- Authorized Users are responsible for logging out of all systems and accounts when they are not being used; they must not be left unattended.
- All laptops and workstations that are part of or connected to the University Information Technology Network are required to be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when the device will be unattended.
- Encryption of information must be used in compliance with Information Security's Acceptable Encryption Use Policy.
- Authorized Users are required to exercise special care to protect laptop computers that are part of or connected to the University Information Technology Network in accordance with the "Laptop Security Guidelines."
- Postings by Authorized Users from a University Email address must contain a disclaimer stating that the opinions expressed are strictly those of the author and not necessarily those of the University, unless posting has been done in the course of University business.
- All computers used by Authorized Users that are connected to the University Information Technology Network, whether owned by the individual or the University,

must be continually executing approved Virus-scanning Software with a current Virus Database.

- Authorized Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain Viruses, e-mail bombs, or Trojan Horse codes.

**Unacceptable Use of the University Information Technology Network**

The following activities are prohibited, although University employees who are Authorized Users may be exempted from these restrictions during the performance of their legitimate job responsibilities. Under no circumstances is an Authorized User permitted to engage in any activity that is illegal under local, state, federal or international law while utilizing the University Information Technology Network.

Unacceptable use includes, but is not limited to the following activities:

**Security and Proprietary Information**

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other Intellectual Property, or similar laws or regulations, including, but not limited to, the installation or distribution of copyrighted or other Software products that are not licensed for use by the University.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted Software for which the University or the Authorized User does not have an active license is strictly prohibited.
- Exporting Software, technical information, Encryption Software or technology, in violation of international or regional export control laws, is illegal. University management must be consulted prior to export of any material that is in question.
- Introduction of Malicious Software into the University Information Technology Network (e.g., Viruses, Worms, Trojan Horses, e-mail bombs, etc.).
- An Authorized User’s revelation of that person’s account password to others or allowing use of an Authorized User’s account by others, including family and other household members when an Authorized User’s computer is connected to the University Information Technology Network from home or other non-University locations.
- The use of a component of the University Information Technology Network or other computing asset to actively engage in procuring or transmitting material that violates sexual harassment or hostile workplace laws or that violates any University policy. Pornographic material is a violation of sexual harassment policies.

- Making fraudulent offers of products, items, or services originating from any University account or otherwise made from a computer connected to the University Information Technology Network.
- Causing Security breaches or disruptions of communication over the University Information Technology Network. Security breaches include, but are not limited to, accessing data or other communications of which the Authorized User is not an intended recipient or logging into an account that the Authorized User is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, Network Sniffing, traffic floods, Packet Spoofing, Denial of Service, etc.
- Port Scanning or Security Scanning is expressly prohibited unless prior notification to Information Security is made.
- Executing any form of Network monitoring which will intercept data not intended for the Authorized User is expressly prohibited, unless this activity is a part of the Authorized User's normal job/duty.
- Circumventing User Authentication or Security of any device, Network, or account.
- Interfering with or denying Service to any user other than the individual's Host (for example, a Denial of Service attack).
- Using any Program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session, via any means locally or remotely.
- Providing information about, or lists of, University employees or Students to non-University parties.

**Email and Communications Activities**

- Sending unsolicited Email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (Email SPAM).
- Any form of harassment via Email, instant messenger, telephone, or pager, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of Email header information.
- Solicitation of Email for any other Email address, other than that of the Authorized User's own account, with the intent to harass or to collect replies.
- Creating or forwarding Chain email, Phishing, or other scams of any type.
- Use of the University's name in any unsolicited Email on behalf of, or to advertise, any service or product without the explicit written permission of the University.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup SPAM).

### *Enforcement*

Any Authorized User found to be in violation of this policy will be considered an Unauthorized User, and as such are subject to disciplinary action pursuant with the Enforcement section of the Unauthorized Use Policy.