Acceptable Use Policy

POLICY: Acceptable Use Policy
Volume: VI
Section: USE OF IT RESOURCES
Responsible Office: CIO
Originally Issued: 12/2013
Revised: 9/2015

I. Policy Statement

Parker University ("Parker") believes that students, faculty, and staff should have the opportunity to become computer literate and should have access to resources that facilitate the ability to connect, create, and collaborate. As a result of this belief, Parker provides computer facilities and information resources to access knowledge and to share that information; supporting the University's mission of education, research, and service. These systems are to be used for educational and business purposes in serving the interests of the University, and of our clients and customers in the course of normal operations.

II. Reason for Policy

The purpose of this policy is to outline the acceptable use of Parker's information resources and to educate applicable parties who may utilize these information resources of their obligations and liabilities accompanying said use. Inappropriate use exposes the University to risks including virus attacks, data loss, compromise of network systems and services, and legal issues.

Information Technology is committed to protecting the University and its employees, faculty, students, partners, patients, and affiliates from illegal or damaging actions by individuals, either knowingly or unknowingly.

III. Policies that work in Unison

Email Policy
Security Assessment Policy
Password Policy
Remote Access Policy
Clean Desk Policy

IV. Policy

a. Definitions

i. **Information resources** in this document are all University-owned, licensed, or managed hardware, software, or data; all computers and devices connected either wired or wirelessly to the campus network, regardless of ownership of the device; and off campus devices that connect remotely to the University's network.

ii. **Users** in this document are all individuals or groups utilizing resources owned or managed by the University; whether networked, individually controlled, shared, or standalone. Users covered by the policy include, but are not limited to, faculty, staff, students, alumni, guests or agents of the administration, external individuals, vendors, and organizations accessing network services.

iii. **Sensitive data** in this document refers to Personally Identifiable Information which might include:
    1. First and/or Last name, Social Security number, Driver's license number, or anything that could be used to aid in identity theft (such as mother's maiden name);
    2. financial data such as Credit card numbers, banking information, tax information;
    3. Federally protected data such as FERPA-protected information (e.g., student information and grades), or HIPAA-protected information (e.g., health, medical, or psychological information);
    4. University restricted or mission-critical data;
    5. Passwords.

b. Scope

i. This policy applies to the use of information resources to conduct University business or interact with internal networks and business systems, whether owned or leased by Parker University, the user, or a third party. All users are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with University policies and standards, and all applicable laws and regulation. Exceptions to this policy are documented in section V.
ii. This policy applies to all users as defined in section **a**.
iii. This policy applies to all information resources as defined in section IV, a, i.

c. General Use and Ownership

i. Parker proprietary information stored on electronic and computing devices whether owned or leased by the University, the user, or a third party, remains the sole property of Parker University. Users must ensure through legal or technical means that proprietary information is protected in accordance with all applicable Parker Policies.
ii. Users have a responsibility to immediately report the theft, loss, or unauthorized disclosure of proprietary University information to the Information Technology department.
iii. Users must immediately report any breaches in Parker computer security. This includes any cases of possible abuse or violation of this or other Parker policies or laws to the Information Technology department.
iv. Users may access, use or share Parker's proprietary information and information resources only to the extent it is authorized and necessary to fulfill their assigned job duties.
v. Users are responsible for exercising good judgment and should limit the amount of personal use of Parker University's information resources.

d. Security, Privacy, and Proprietary Information

i. All users utilizing mobile computing devices that connect to the internal network must comply with all applicable Parker policies as well as applicable laws and regulations.
ii. Users are encouraged to make frequent backups of important or sensitive data in an appropriate and secure manner to Parker-provided

storage devices. Parker IT has measures in place to prevent data loss, however, hardware or software failure can occur at any time which may result in data loss. Parker is not responsible for any damages caused by any data loss due to hardware or software failure or deletion.

iii. System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

iv. Users must use extreme caution when opening all e-mail attachments, which may contain malware. Users are encouraged to only open attachments from trusted sources from which they were expecting an email.

v. For security and network maintenance purposes, authorized individuals within the University may monitor equipment, systems, and network traffic at any time, per Information Technology's *Security Assessment Policy*.

vi. Parker Information Technology reserves the right to audit networks and systems at any time to ensure compliance with this and all other Parker policies.

e. Unacceptable Use

The following activities are, in general, prohibited. Users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may be required to disable the network access of a host if that host is disrupting production services).

Under no circumstances is a user of the University's information resources authorized to engage in any activity that is illegal under local, state, federal, or international law or in violation of any University policy while utilizing Parker-owned information resources. Examples of applicable laws and policies include, but are not limited to:

- Health Insurance Portability and Accountability Act (HIPAA)
- The Family Educational Rights and Privacy Act (FERPA)
- Payment Card Industry standards
- The Electronic Communications Privacy Act
- The Computer Fraud and Abuse Act
- The Americans with Disabilities Act
- Parker's Employee Handbook
- Parker's Student Handbook
- Parker's Code of Student Conduct
- Parker's Sexual Harassment Policy
- Laws and policies governing libel, harassment, privacy, copyright, trademark, obscenity, and child pornography
- Software license Agreements
- Users engaging in electronic communication with persons or groups in other countries, states, university systems, or networks may be held liable for violations of the laws, rules, and policies governing said external entities. Users are responsible for understanding and complying with all applicable laws, rules, or policies.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of ***unacceptable*** use.

i. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. 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 "pirated" or other software products that are not appropriately licensed for use.

2. 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 end user does not have an active license.

3. Accessing data, a server, or an account for any purpose other than conducting University business, even if you have authorized access. The ability to access a resource does not, on its own, suggest approval to do so. Users are responsible for obtaining proper authorization prior to accessing any University resources and utilizing them only within the boundaries authorized.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a Parker information resource to actively engage in procuring or transmitting material that is sexually explicit or in violation of sexual harassment or hostile workplace laws.

8. Making fraudulent offers of products, items, or services originating from any Parker account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly

authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to Information Security is made.

12. Executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the user's normal job/duty.

13. Circumventing user authentication or security of any host, network, or account.
14. Introducing honeypots, honeynets, or similar technology on the University network.

15. Interfering with or denying service to any user other than the user's host (for example, denial of service attack).

16. 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 via the Internet/Intranet/Extranet.

17. Providing information about, or lists of, Parker users to parties outside of the University.

ii. Email and Communication Activities

1. When using company resources to access and use the Internet, users must realize they represent the company. Whenever users state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

2. 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).

3. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

4. Unauthorized use, or forging, of email header information.

5. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

6. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

7. Use of information resources for commercial purposes or other personal gain. Accounts and information resources may not be used for commercial or personal activities other than Parker-sanctioned business. Examples include, but are not limited to, consulting, computing for commercial organizations, advertising, soliciting, fundraising, or proselytizing for commercial ventures, religious or personal causes.

iii. Blogging and Social Media

1. Blogging or social media use by users, whether using Parker's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of University systems to engage in personal social media is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Parker's policy, is not detrimental to the University's best interests, and does not interfere with an user's regular work duties. Blogging and social media use from Parker's information resources is also subject to monitoring.

2. All Parker policies regarding confidential information also apply to social media and blogging. As such, Users are prohibited from revealing any University confidential or proprietary information, trade secrets or any other material when engaging in blogging, social media, or any other form of communication.

3. Users shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the University and/or any of its users. Users are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when blogging or otherwise engaging in any conduct prohibited by Parker University policies or handbooks.

4. Users may also not attribute personal statements, opinions or beliefs to Parker University when engaged in social media. If a user is expressing his or her beliefs and/or opinions in blogs, the user may not, expressly or implicitly, represent themselves as an user or representative of the University. Users assume any and all risk associated.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Parker University's trademarks, logos and any other University intellectual property may also not be used in connection with any personal blogging or social media activity

V. Procedures

a. Scope

This policy is applicable to all users utilizing any and all information resources as defined in section (IV, a).

b. Compliance Measurement

The Information Technology department and Information Security team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

c. Exceptions

Any exception to the policy must be approved by the Chief Information Officer in advance.

d. Non-Compliance

Violation of this policy may result in disciplinary action, up to and including termination for permanent and temporary employees; a termination of employment contract in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Parker University Information Resources access privileges and to civil and criminal prosecution.

The use of information resources should be viewed as a privilege and, as such, privileges may be revoked for violations either deliberate or accidental. Parker reserves the right to restrict or revoke access to any user who misuses, or is suspected of misusing, any information resource, violates any applicable Federal or State law, any of these terms and conditions, or otherwise abuses their privilege to use the computer facilities. The University may also refer violations to appropriate law enforcement agencies. If a student's access rights are revoked due to infraction of applicable Federal or State law, this or other University policies, the student is required to continue payment of the Technology fee as long as they remain a student at Parker University.

VI. Contacts

Please direct questions and report any violations of this policy to the Chief Information Officer.

Approved by* Cabinet*: 9/2015