

policy or agreement stating otherwise. As a result, users should not expect any personal privacy for

Subject: Network Services**Policy**

JU makes a wide variety of network services available from email to online network storage. Users should consult the list of network services by visiting the IT website; <http://it.ju.edu>.

1. Internet Gateway ernet. This very popular resource is limited in its ability to handle traffic. To ensure equal access for all, certain types of traffic may be rate limited or even blocked periodically. Peer-to Peer traffic is always blocked.

2. Network Maintenance: JU reserves the right to take down network services for maintenance without notice. Planned maintenance that will impact services over a long period of time will be announced prior to the event via JU email. Planned maintenance that will impact services for less than 15 minutes will not be announced, however, all efforts will be made to accomplish the maintenance after classes complete for the day. IT constantly monitors the network for performance and security reasons. Automated devices are used as well as manual means. Selected individuals in the IT Department have full access to University owned systems in order to fulfill the requirements of their job. Information transmitted over the network or stored on university owned computers may be viewed by those individuals during the performance of their duties.

Subject: Policy Review**Policy**

These policies will be reviewed and revised annually reflect changes to technology. Suggestions and proposed changes to the policies should be submitted to the Chief Information Officer. Changes to the policy shall be approved by the Chief Information Officer.

Subject: Students; Overview**Policy**

Jacksonville University provides and supports technology across campus and across the Internet to support students in their pursuit of a college degree. These policies apply to all current, former, and prospective students. JU provides computers throughout campus for use by the students in open labs and classrooms. These computers are configured to provide students with services tailored to the tasks needed to assist them with their studies. Additionally, students living on campus are provided access to the campus Internet gateway from their residence.

The network at Jacksonville University consists of computers, networking devices, telecommunications systems, and the Internet gateway. The primary purpose of the network is to support the mission and ongoing business of the University. Access to and use of the network is a

Students may not use the network for personal financial gain.

Switches, routers, hubs, and wireless access points are prohibited. If these devices are detected, the

two-

person room may use both network ports in that room.

Subject: Faculty/Employees; Donated Items

Policy

In addition to the requirements set forth in section 700; Developmental Fundraising, accepting donations of IT related equipment such as computer systems, printers, PDAs, smart phones, etc., without approval of the Gift Acceptance Committee is prohibited.

Subject: Faculty/Employees; Personally, Owned Equipment

Policy

University. As such, it does not provide support or assistance with personally owned equipment. Employees may not bring personally owned computers on campus for business use. Employees required to work from home should have their supervisor contact IT for information on the approved methods for telecommuting. Employees desiring to use their personally owned tablet or smart phone to check their JU email and calendar may do so with the understanding that their device will require a self-assigned passcode every time they use it. IT will provide the information required to connect to these services but will not set the device up. The employee is responsible for providing his/her own support. Requests for software installation on JU computers for support of a personally owned device must come from the supervisor. All configuration, operation and support of this software are the responsibility of the employee.

Subject: Faculty/Employees; Administrative Rights

Policy

This policy addresses the voluntary use of the University's electronic resources and the internet via the University's network to provide guidance to faculty and staff. Every member of the University community is covered by this policy and expected to be familiar with its provisions. We recognize the value of computer and other electronic resources to enhance the administration and operation of the University. To this end, we encourage the responsible use of computers, computer networks, including the Internet, and other electronic resources, which must be in support of educational and research objectives consistent with our mission and goals. Use of our electronic media offers a wealth of information and resources for research. ***In addition, users are expected to exercise good judgment in interpreting these guidelines and discretion in making decisions about the appropriate use of our resources. Any person with questions regarding the application or meaning of these guidelines should seek clarification from the Information Technology Department.***

Monitoring and Privacy. It is the University's policy to maintain an environment that promotes ethical and responsible conduct in all network activities, including activities on the Internet and the privacy of others. However, we need to monitor network activities to maintain network security and for other lawful reasons. The University retains the right to inspect your hard drive and the files it contains. In addition, an Internet firewall automatically checks all data moving between the local area network and the internet and logs the sending and receiving destinations.

Use of the University's technology resources constitutes consent for the information technology and other administrative staff to monitor and/or inspect any files that users create, any messages they post or receive, and any web sites they access. Please remember that you have no expectation of privacy. Among the things we may do to ensure compliance, we may log network use and to monitor fileserver space utilization by users. We assume no responsibility or liability for files deleted due to violation of fileserver space allotments. We may also monitor the use of online activities. This may include real-time monitoring of network activity and/or maintaining a log of Internet activity for later review. You are advised that messages in discussion forums, including deleted messages, are regularly archived, and can be retrieved. It is a violation of this policy to engage in any activity that does not conform to the University's established purpose and general rules and policies regarding use of the network.

The University reserves the right, in its sole discretion, to request an explanation and justification regarding any hardware or software not provided by the University's Information Technology Department that is installed on any computer or the network, and at any time to remove the hardware or software from the computer (or the network). It is each user's responsibility to ensure that no one is granted access to the network via the user's computer and that only you have access via your account.

Compliance. Each of us must exhibit exemplary behavior on the network and the internet as a representative of the University community. Good judgment by each of us is primary in maintaining control of the use of our resources; however, we will provide internal and external controls as appropriate and feasible. The controls include the right to determine who is granted access to University-owned equipment and, specifically, to exclude those who do not abide by this or other applicable policies. The University reserves the right to restrict online destinations through software or other means.

From time to time, the University may make determinations on whether specific uses of the network are consistent with University policies. Any use of the network for any purpose that is contrary to University policy is prohibited. Malicious use of the network to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system is prohibited. Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials (including unauthorized copies of software) without the specific written permission of the copyright owner is prohibited, except that duplication and/or distribution of materials for educational purposes is permitted when the duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law. The network may not be used for downloading software or other files not related

to our mission and objectives or for transfer to other computers, personal computer, or

Using the 25Live System to Request Technology Support for Events. When you request A/V or technology support for an event via 25Live, the help desk is contacted on your behalf during this process, so a duplicate request is not necessary.

Subject: Requesting IT Assistance

Policy

All requests for IT services and support must be initiated through the Help Desk. Requests should not be made directly to members of the IT Department.

Subject: Printer Support

Policy

DELL LASER PRINTERS

Dell laser printers are maintained by Saxon Business Systems. If the printer needs to be serviced or

DELL LASER MULTIFUNCTION PRINTERS

All Dell laser multifunction printers purchased through the IT department have a 3-year warranty from the manufacturer. If the printer needs to be serviced or repaired and is out of warranty, the IT department will evaluate the costs of service or repair and inform the user or department if a new printer purchase is a more cost effective solution. All printers that are still under warranty will be repaired by the IT department if required. Servicing the printer such as new toner, cleaning, fuser replacements, etc, are not covered under the manufacturer warranty and these costs will be covered by the department that owns the printer. The IT department will always help the user or department troubleshoot any printer issues with software or connectivity.

INKJET PRINTERS AND INKJET MULTIFUNCTION PRINTERS

The IT department does not service or repair InkJet printers. Any service or repair will have to go through the manufacturer. The IT department can evaluate the printer and inform the user or department if a new purchase would be a more cost-effective solution in any situation. IT will help the user install the necessary software and verify that a test page can be sent to the printer. However, any printer problems that seem to be related to the printer itself will not be analyzed or repaired by the IT department.

MULTIFUNCTION CORPORATE PRINTERS/COPIERS Konica Minolta/Xerox

These systems are maintained by Dex Imaging (Konica Minolta) and Saxon Business Systems (Xerox)

Subject: Backup & Retention

Policy

The process to backup digital communications, data and other electronic files is an essential IT practice to insure against the loss of valuable information. The purpose of backing up the stored data is to allow the university to restore a system to a current state, in case of a system failure, or to restore individual files inadvertently deleted or lost. The backup media is not intended to serve as a short or long-term storage information vault.

The purpose of this policy is to establish a limit on the length of the time backups are maintained and to encourage departments to distinguish between the purposes and practices of backing-up data vs. the retrieval (archive) of data.

Email and File Backup Policy

ain data long enough to provide a reasonable level of insurance against major data losses. Procedures will be based on the nature of the data, the volatility of the data, etc., and will be carefully coordinated with retrieval storage practices (All departments will have their own procedures on the way they keep their data for archiving/compliance).

(Office 365) is not backed up. Email deleted from employee accounts will be recoverable for a period of 60 days. Email deleted from non-employee, student and alumni accounts will be recoverable for 14 days.

files including Microsoft Office 365 OneDrive for Business should be retained for no

Policy**Purpose:**

The purpose of this policy is to provide guidance for employees choosing to use social media to communicate, collaborate, and interact with students, faculty, staff, stakeholders, and the general public on matters concerning or impacting Jacksonville University.

Scope:

This policy applies to Jacksonville University employees representing JU or its programs in an official capacity who create or contribute to blogs, wikis, social networks or any other kind of social media (both on and off JU.edu). These guidelines also apply to other people (such as volunteers and appointees) who use internally managed university computing resources. This policy applies to all forms of social media, including, for example, Facebook, Twitter, Instagram, Snapchat, YouTube, LinkedIn, blogs, online comments, etc. This policy may apply to employees outside of work hours and while using personal accounts when use of social media affects an

JU regulation or policy. Your online persona, and the content you publish, should be consistent professional standards.

Policy Statement:

Jacksonville University is committed to the highest standards of freedom of speech and expression. JU recognizes the vital role that social media can play in both expressing free speech and also in communicating, collaborating, and interacting with students, faculty, staff, non-JU colleagues, and the general public.

This policy intends to protect the appropriate use of social media, while prohibiting conduct through social media that may be unlawful, violative of professional standards, contrary to the University mission, policies, and its culture of respect for all individuals.

Procedures:

During working hours, JU employees may not spend more than minimal work time on personal activities, including the use of social media. Use during breaks and meal period is permitted. In some supervisors may author hng wor0912 0 612 792 reW*nBT/F1 12 Tf1 0 0 1 72.025 227.33 Tm0 g0 GcdQ E

exercise caution with regards to exaggeration, obscenity, guesswork, copyrighted materials, legal conclusions and derogatory remarks or characterizations.

3. If you discuss work-related matters online that are within your job responsibility, must disclose your affiliation with the University.

4. You may not disclose any sensitive, proprietary, confidential, legal or financial information about the University or individuals affiliated with the University. You may not disclose information protected under FERPA, HIPAA, or other laws or regulations.

5. While you may respectfully disagree with the University actions, policies or leadership decisions, you may not attack personally or post material that is obscene, defamatory, discriminatory, harassing, libelous or threatening with regard to the University, employees of the University or any affiliates of the University.

6. All Jacksonville University social media accounts must be registered with University Communications and follow Jacksonville University brand guidelines. Please consult with Human Resources if you have any questions about the appropriateness of publishing information relating to the University, its faculty, staff or any affiliates.

For consideration: Possible hyperlinks, relevant policies to consider including

- ◁ State and federal laws regarding privacy, defamation, copyright