# FAULKNER UNIVERSITY

## USE OF COMPUTING AND INFORMATION TECHNOLOGY RESOURCES

| | |
|---|---|
| Section: **Administrative - Finance** | Effective: **September 1, 2007** |
| Policy Number: **455** | Revised: **September 18, 2017** |
| Past Revisions: **June 28, 2011; June 27, 2012; Sept. 29, 2014** | Reviewed: **September 2017 DB/BP** |

**Purpose:** To establish the policies, procedures and practice for the University's information technology services and resources. These rules are in place to protect the student, the employee and Faulkner University. Inappropriate use exposes Faulkner University to risks including virus attacks, compromise of network systems and services, and legal issues.

**Scope:** This policy applies to students, employees, contractors, consultants, temporary/adjunct employees, and other workers at Faulkner University, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Faulkner University and those utilizing the University's network.

### SECTIONS OF THIS POLICY

### 1. GENERAL INFORMATION

Faulkner University's computing, information technology and network resources are provided to students and employees for the purposes of study, research, service and other academic and administrative related activities. Faulkner's information system facilities are a valuable resource, and they must be used in a responsible manner.

All University-owned computing systems, including but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Faulkner University and 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, and must be used in accordance with all University policies. All electronic files and records utilizing University resources are the property of the University and may be copied, reviewed, audited, distributed, etc. as deemed necessary by the University.

Any individually assigned University-owned computing equipment including, but not limited to, desktop computers, laptops, iPads, and smartphones, must be returned to the University upon termination of employment.

Employee and student access to Faulkner's information facilities is a privilege, not a right. All users must agree to use the facilities legally, ethically, and in keeping with their intended use.

## 2. ADMINISTRATION

Under the supervision of the Vice President for Finance, EFC Systems serves as the System Administrator and oversees the daily operations of the University's networks, websites and resources. The Vice President for Finance must approve all system enhancements and hardware purchases, in keeping with Policy # 440, "Purchasing and Expense Reimbursement."

The University Technology Committee serves as an advisory body to the administration. The Vice President for Finance serves as Committee Chair. In collaboration with other administrative officials, this individual appoints members, leads the committee and can appoint sub-committees to accomplish various tasks as approved by majority.

## 3. ACCEPTABLE USE AND ETHICS

Technology resources at Faulkner University require strictly legal and ethical utilization by all users. These resources are limited and should be used wisely and carefully. The following list, though not intended to cover every situation, specifies some of the responsibilities that accompany usage of Faulkner computing facilities and the networks of which Faulkner is a member. All users are expected to abide by these regulations. Employees and students must sign a form stating understanding of the university computer policy.

All Faulkner rules of conduct, as outlined in other policies and handbooks, apply when using Faulkner's technology resources. Questions concerning ethical or legal use of these resources should be directed to the System Administrator.

3.1 All users are responsible for ensuring that what they do is legal. Users are prohibited from any practice or user activity that, in the opinion of the University Administration constitutes irresponsible behavior, promotes illegal activities, results in the misuse of computer resources, or jeopardizes the operation of computer or network systems.

3.2 Technology resource usage must be consistent with the goal of facilitating the exchange of noncommercial information in support of Faulkner's mission of education. Resources must not be used for commercial purposes or monetary gain.

3.3 Users must respect the privacy of others. Users must not search for, access, or copy directories, programs, files, disks, or data not belonging to them unless they have specific written authorization to do so. Programs, subroutines, and data provided by Faulkner may not be taken to other computer sites without written permission from the Vice President for Finance. Users may not use programs obtained from commercial sources or other computer installations unless written authority to use them has been obtained from the Vice President for Finance. Users may not use Faulkner computer equipment or software in violation of the terms of any license agreement.

3.4 Users are prohibited from physical or electronic interference with others' use of the computer resources. This includes such activities as tying up computer resources for game playing or other trivial applications; leaving internet browsers open for extended periods of time (i.e. listening to a ballgame or radio via the internet); sending frivolous, excessive, or unwanted messages or email, either locally or over the networks; forging email or credentials; using excessive amounts of storage; and printing excessive copies of programs, files or data.

3.5 Users must not attempt to modify or crash any computer system, nor attempt to modify the restrictions associated with the user's computer login ID and password. Users must not attempt to repair, disconnect, or remove any University-owned computer or computer equipment.

3.6 Users must not conceal their identity when using Faulkner computing facilities, except when anonymous access is explicitly provided.

3.7 Users are prohibited from accessing, transmitting, receiving, displaying, viewing or storing offensive content, which includes, but is not limited to, sexual comments or images, racial slurs, gender specific comments or any comments that would offend someone on the basis of their age, sex, national origin or disability. Users are prohibited from displaying, sending, printing, or storing sexually explicit, graphically disturbing, obscene, pornographic, fraudulent, harassing, threatening, abusive, racist, or discriminatory images, files or messages utilizing any University computing facility or resource or in any campus location.

3.8 Computer users are prohibited from using University computer resources to conduct computer harassment. Computer harassment includes, but is not limited to:

3.8.1 Text and images sent with the intent to harass, terrify, intimidate, threaten or offend another person;

3.8.2 Intentionally using the computer to contact another person repeatedly with the intent to harass or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease;

3.8.3 Intentionally using the computer to disrupt or damage the academic, research, administrative or related pursuits of another; and

3.8.4 Intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

3.9 Users are prohibited from storing, transmitting, disseminating or printing copyrighted materials, including computer files, articles and software, in violation of copyright laws, or engaging in any other activity in violation of any federal, state, or local laws, including copyright law.

## 4. ACCESS, SECURITY, AND PRIVACY

The University employs various measures to protect the security of its information resources. Users should be aware that their uses of University computer and network resources are not private. While the University does not routinely monitor individual usage, the normal operation and maintenance of the University's computing resources require backup, logging of activity, the monitoring of general and individual usage patterns, and other such activities that are necessary for information security and the rendition of service. In addition, the University reserves the right to review, monitor and/or capture any content residing on, or transmitted over, its computers or network at its sole discretion. The University reserves the right to limit access to its computers or network, and to remove or limit access to material residing on its computers or network.

Effective security requires the participation and support of every Faulkner University student, employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

### 4.1 Passwords

Users must use ONLY the login ID and password that has been authorized for their use. Passwords must not be shared with others and users must not log into the system under someone else's user name. Users are responsible for everything done on their password. If access is needed to an area, a request for change in security access should be submitted to the System Administrator. Passwords must be changed immediately if disclosed or compromised.

All Faulkner users will be required to generate a password for network logon that conforms to the following criteria:

1. Does not utilize the user's account name as any portion of the password
2. Must contain at least 6 alphanumeric characters
3. Must contain at least one character from three of the following four options:
   - Uppercase letter (A-Z)
   - Lowercase letter (a-z)
   - Number (0-9)
   - Special Character (!, @, #, $, %, ^, &, *, +, =, ?)
4. Has not been used within the previous 12 months

Users should avoid using their names or the names of their spouse, children or friends; birthdates; or any other password that could easily be guessed.

Faulkner users will be required to generate a new password twice yearly. Users will begin being prompted to change their passwords 14 days prior to expiration at which point they will be forced to change their password.

Faulkner accounts will allow 5 invalid login attempts prior to the account being locked. Locked accounts will remain locked for 30 minutes. EFC may be contacted to manually override a locked account.

Faulkner user accounts that have not been logged on for the previous 365 days will be locked until a new password is generated. Password recovery can be completed by contacting EFC and providing verification of identity.

### 4.2 Access to Data and Privacy Rules

All computer and electronic files should be free from access by any but the authorized users of those files. Access to institutional data shall not be granted to persons unless there is an established business need to know.

All educational records maintained on the University's administrative servers and/or REGENT system are subject to the rights, responsibilities and limitations of the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99). All computer users are responsible for reviewing the University's FERPA policy.

All employee and student health and counseling records are subject to federal and state regulations "privacy rules" including Health Insurance Portability and Accountability Act (HIPAA), 42 USC 290dd-3 and 42 USC 290ee-3. All computer users are responsible for reviewing the University's HIPAA policy.

### 4.3 Computer Desktop and Workstation Security

Access to all Faulkner computer desktops and stations will require the use of a Faulkner logon ID and password. Computers that are logged into the network should never be left unattended. Users should perform a screen lock whenever they will be leaving their computers unattended for a short period of time in order to prevent unauthorized access to their systems.

Faculty and staff desktop computers will require a secure logon after 15 minutes of inactivity. After 15 minutes of inactivity, a keyboard lockout will be applied; all open documents, files, will not be affected.

### 4.4 Logging In and Out / System Shutdown

REGENT users should completely log out of REGENT when leaving for lunch or an extended period of time, and at the end of the workday as computer service personnel may need to bring the system down for routine maintenance while an employee is out of the office.

### 4.5 Power Failure

When power failure occurs, the user should immediately log out and shut down the system properly. This means if working in REGENT, the user should log out of REGENT properly. If working in applications other than REGENT, users should immediately save files. Once

REGENT and other applications have been saved and properly closed, users should then shut down the computer system properly and power off all equipment. Users should wait for verification from EFC before attempting to log back onto the system.

### 4.6 REGENT Access

Regardless of security restrictions, employees or students are not to access any REGENT module that is not necessary to that individual's daily operations. Security breaches must be reported immediately to the System Administrator.

Changes in a user's REGENT security must be submitted on a CHANGE OF JOB/STATUS FORM, and must have appropriate supervisor and Vice-Presidential approvals. The System Administrator must approve all system access change requests.

### 4.7 Remote Network Access

Remote access to the University's network is governed by policy #454, "Remote Network Access." This policy applies to all faculty, staff, contractors, vendors and agents utilizing University-owned or personally-owned computing devices, including but not limited to desktop computers, workstations, laptops, iPads, Smartphones, and tablet computers to connect to the University's network. This policy applies to all connections to devices on the network (including servers and desktop computers) originating from devices outside the network.

### 4.8 Removal of Network Access

In the case of employee termination, the System Administrator should be contacted immediately to initiate appropriate system security changes. Unless otherwise authorized for an extension, network access for employees terminating from University employment will be removed as of the employee's last working day. The University reserves the right to remove or limit an employee's network access at any time deemed necessary for the security of the University's data and assets.

EFC personnel will remove all student accounts from Active Directory (this is the account that students use to login to their account on the web or access their email) if the student has not had any class time in four months or more.

In the case of student withdrawal, graduation or other discontinuance of enrollment, the System Administrator should be contacted immediately to initiate appropriate system security changes.

### 4.9 Security Breach

In the event of a known or suspected security breach, the System Administrator should be contacted immediately, along with the department supervisor and the Vice President for Finance. The individual allowing, causing, committing, or otherwise responsible for a breach of security, will be subject to institutional disciplinary proceedings and, if applicable, civil and/or criminal legal proceedings.

### 4.10 Service Requests

Services requests are to be submitted via e-mail to "Helpdesk." Requests should include as much detail as possible. Do not send duplicate requests. Clarification, explanation, and follow-up may be accomplished by telephone.

Appropriate supervisor must approve requests for REGENT software changes.

If a major computer problem occurs after hours, refer to contact information in the labs. Employees should contact the afterhours help number however this number should not be given to students.

## 5. EMAIL AND TEXT MESSAGES

All university e-mails are considered records of Faulkner University, and therefore cannot be considered private. Email and text messages sent by means of an employee's personal cellphone in the context of University business are also considered records of Faulkner University and therefore cannot be considered private. Messages may be monitored or obtained in cases where a legitimate business need is present.

- E-mail is to be used primarily for official university business and should not be abused or misused.
- E-mail messages are considered official communication by Faulkner University and can be relied upon as a means of communicating vital information.
- E-mail users should be aware of the University organizational chart and observe the chain of command, just as when making a phone call or visit.
- The "Main Campus" e-mail group is moderated in order to keep communications professional, pertinent, and efficient. E-mail is a work tool, and users do not want to spend time sifting through e-mail that is not job-related. A "Bulletin Board" is available under Google Groups for posting general messages and emails of interest.
- E-mail and text messages should not contain inappropriate, disruptive, threatening, or offensive language. Users should avoid slander and libel, chain letters and pyramid schemes, and all other questionable email and text messaging activities.
- E-mail messages can be traced back to Faulkner University. Employees should keep this in mind before sending messages to the community.
- E-mail messages are not to be sent on someone else's login credentials. Users must not attempt to forge of email messages.
- Messages that have been place in "Trash" for 30 days will be deleted permanently. There is no mailbox size limit for students or faculty/staff.

## 6. INTERNET USAGE

The Internet should be accessed primarily in relation to work at Faulkner University and should not be abused or misused. Supervisors will be responsible for monitoring employee Internet usage, just as they would monitor any other activity during work hours.

Users should be aware that Internet access produces a traceable log file of all sites visited by that user's ID, how frequently these sites were visited, including how long the site remained open. In addition, EFC personnel have been instructed to randomly monitor Internet usage. Because of the seriousness of abuse findings, the importance of not loaning the user ID and password to others must be stressed.

## 7. UNIVERSITY WEBSITE

The Faulkner University website (www.faulkner.edu) is an official means of communication for the University to inform students, alumni, faculty, staff and the general public of mission critical information. Content is provided by authorized personnel who have been granted permission by a Dean or Vice President. Authorized personnel must receive training before removing, adding, or changing content.

Faulkner University web content may only be edited using the tools and/or methods provided by the University according to the rules and guidelines set forth by the University. These guidelines are documented in the Style Guide and can be obtained by sending a request to "Webmaster." Faulkner webpages should be monitored routinely to ensure posted data is current.

Requests for custom web-based applications must be approved by a Dean or Vice President and submitted to the webmaster at least 30 business days before the needed deadline. All requests are subject to approval and Faulkner University reserves the right to remove any material, or any links to material, from Faulkner University webpages.

Web pages are not to be created using Faulkner's name or logo without prior approval from the Website Committee.

## 8. OTHER SOFTWARE

Non-standard software to be loaded onto the networks or local hard drives must be approved by the System Administrator before being loaded. Requests for approval are sent to Helpdesk. EFC will check into the compatibility of the program before software is loaded onto the network or local hard drive. Purchased software must contain adequate licensing to cover all potential users.
Computer games, videos, and/or music are not to be loaded onto University computers except for educational purposes.

In order to prevent the spread of computer viruses, users should not use electronic storage devices such as flash drives to transfer files between the student computer labs and the administrative network.

## 9. COPYRIGHT OBSERVANCE

All users of Faulkner University-owned computing devices and networks are to abide by copyright laws and licensing agreements. No software should be loaded on any Faulkner computer in violation of licenses or laws. Copyrighted software must only be used in accordance with its license or purchase agreement. Users do not have the right to receive and/or use unauthorized copies of software, or make or attempt to make unauthorized copies of software for themselves or others. All computer users must comply with the Digital Millennium Copyright Act (DMCA) (Public Law 105-304).

In addition to federal and state laws prohibiting the theft of software, Faulkner prohibits copyright or licensing infractions from or on any component of Faulkner's systems. Faulkner University will not be liable for copyright or licensing infringements by any student, faculty or staff member.

### 9.1 Definition of copyrighted material

Materials or “works” that fall under copyright law protection are basically defined as: text, images, music, movies, or other performances that have been created by an entity, and have been fixed in a copy (on paper; example: sheet music), or phonorecord (on media; example: CD, cassettes, or LPs). A “work” that has been created is automatically copyrighted upon its creation. It is not necessary to register a “work” with any official office, add a symbol or otherwise report or request a copyright from any federal or state office or service.

Copyrighted material cannot be copied or stored (unless a license or permission has been granted by the copyright owner) on any type of media, including but not limited to, a hard disk, removable media (such as USB drives, ZIP disks, and CD-Rs), a network storage location, or on physical media (paper print-outs) by anyone other than the copyright owner, or an authorized agent of the copyright owner.

### 9.2 Enforcement and Penalties

Faulkner University reserves the right to examine all computer files stored on University-owned computing devices. If questionable materials are found, they will be immediately removed, or access will be disabled, and a notice will be sent to the user. If the user has a license, or has received permission from the copyright owner to possess the material, the user must submit a counter notice as pursuant to 17 U.S.C. 512(g)(3), to the office of the Vice President for Finance that the removal or disabling of access was based on a mistake or misidentification. If the materials are found to be of a legitimate origin, the materials will be replaced or access will be restored in 10 to 15 business days.

If a user is found to have violated copyright law, and this policy, Faulkner University may decide to take disciplinary action against the user. There may also be civil and criminal penalties as dictated by a court of law.

## 10. LIABILITY

Faulkner University hereby expressly and explicitly disclaims any liability and/or responsibility for violations of the policy stated above.

## 11. VIOLATIONS

Any individual allowing, causing, committing or otherwise responsible for a violation of this computer policy, will be subject to institutional disciplinary proceedings and, if applicable, civil and/or criminal legal proceedings. (It should be understood that this policy does not preclude enforcement under the laws and regulations of the state of Alabama and the United States of America.)

Inappropriate use of Faulkner computing facilities may result in cancellation of computing privileges. Faulkner University reserves the right to examine all computer files.

In the case of an employee violating the policy, the immediate supervisor will initiate employee disciplinary proceedings.

In the case of a student violating the policy, the Dean of Students or other appropriate University official will initiate Student Life disciplinary proceedings.

In the case of a student who is also an employee violating the policy, the Dean of Students or other appropriate University official will initiate Student Life disciplinary proceedings and the immediate supervisor will initiate employee disciplinary proceedings.