



Network and Responsible Computing Policy

School-provided technology resources – including, but not limited to, computers (eg, desktop and portable computers, servers, networks, printers, software and data storage media), email, and Internet use (collectively, technology resources), are available for exclusive use of authorized, registered students, faculty and staff (“users”). To better serve the needs of users and emulate an academic university computing environment, the following policies are enforced by the Help Desk and Information Technology (IT) staff. Users must familiarize themselves with and abide by the following policies:

A. Network and Workstation Security is Strictly Enforced

Users have no expectation of privacy in connection with use of the University’s technology resources, including creation, entry, receipt, storage, access, viewing, or transmission of data. The University, through the IT Department or Help Desk staff, may search, monitor, inspect, intercept, review, and/or access all data created, entered, received, stored, accessed, viewed, or transmitted on or through the University’s technology resources, or other University-provided technology to maintain system integrity and insure users are using the system responsibly.

The IT staff may also implement workstation management software, allowing them to monitor for or prevent users from attempting to change settings or circumvent workstation security.

Users may not attempt to alter workstation settings including, but not limited to, network configuration, Windows® registry, virus checker settings or any other setting that might compromise security or performance of the University computer system. The IT Department may implement workstation security software to monitor for, and/or prevent users from making, inappropriate changes to their workstations.

Any attempt by a user to breach workstation or network security, or to tamper with University technology resources, will result in loss of computer access. Downloading material relating to hacking or malicious code creation will be considered an attempt to breach network security.

Further disciplinary action may be pursued as described below in Section E.

B. Guidelines for use of the University’s technology resources

1. The privacy of other users must be respected.
2. Users are responsible for all activities conducted under their user login and password, whether intentional or unintentional, on the University’s technology resources.
3. Students will not use the University’s technology resources to intentionally or unintentionally violate any local, state, federal, or international civil or criminal law. This includes:
 - Making statements or transmitting data threatening, malicious, tortuous, defamatory, libelous, vulgar, obscene, or invasive of another’s privacy.
 - Violating copyright, trademark, patent or any other intellectual property laws. This would include transmitting, posting or copying another user’s work without express consent of the intellectual property owner.
 - Running or participating in lotteries, raffles, betting, gambling for anything of value and participating or facilitating in the distribution of unlawful materials.
 - To gain unauthorized access to other computers or databases not in the public domain.
 - Users of the University’s technology resources should abide by the same principles of fairness, decency, and respect that would be expected in any other school or business environment.
 - Users are forbidden from using the University’s technology resources in any way that may be reasonably construed to violate the University’s policies, including its no-harassment policies. This prohibition includes, but is not limited to, sexually explicit or offensive images,

messages, cartoons, jokes, ethnic or religious slurs, racial epithets, and using abusive and offensive language.

- Computer technology resources may not be used to transmit junk mail, SPAM, pyramid schemes of any kind or chain letters.
- Users must minimize the possibility of transmitting viruses or programs harmful to another user's data or equipment by using an appropriate virus checker.
- Users may not install, store or download software programs or hardware on University computers. Any unauthorized software or hardware modifications will be removed.
- Off-campus websites and email accounts created or accessed over the University computer network are subject to these policies and regulations.

C. User accounts are available for academic purposes only

All technology resources are intended for educational use and may not be used for commercial or other unauthorized purposes. Use of University technology resources – including computers, network facilities, application software, network disk space and the Internet – are available for the purpose of coursework and support only. Communication using technology resources is available for authorized users only.

Students are issued an account when they appear on the official class roster. All accounts are for the exclusive use of the person to which they are assigned and may not be "loaned" to anyone. Other types of accounts may be applied for by completing an Account Request form at the Help Desk. A Help Desk assistant will check the user's ID and sign the form indicating the ID was confirmed. All users are given their own space on the network hard drive for storing course-related material and assignments. They may also receive access to specific software packages based on the judgment of the network administrator.

All passwords expire every 90 days. Ross reserves the right to withdraw access to facilities or network from **any** user and all rights to **any** material stored in files and will remove **any** harmful, unlawful, abusive or objectionable material.

Ross does not guarantee functioning of the system will be error-free or uninterrupted. In addition, students are responsible for backing up all their electronic files. The University is not responsible for student files.

D. Food and beverages are not permitted in labs

Food particles and liquids easily damage computer equipment, making systems unavailable and raising costs to users. For example, soda and coffee damage the printed electrical traces of a keyboard on contact, and food crumbs clog mice and keyboards. Therefore, food and beverages are prohibited in computer labs.

E. Violations of these policies may result in accounts being disabled and further disciplinary action deemed appropriate

Access to and use of the University's technology resources is a privilege, not a right. Users who do not comply with these policies are subject to denial of access to University technology resources and disciplinary action. The University may amend, revise or depart from this policy at any time, without prior notice.

Users who have their accounts disabled should contact the Help Desk to find out whom to contact to regain computer access. Minor violations may be resolved by the IT Department or Help Desk.

Major violations will be referred to the Student Services Office for further action under the *Student Handbook*, as described below. (Other portions of the *Student Handbook* may also apply, depending on the nature of the violation.)

F. Unauthorized Distribution of Copyrighted Materials

Ross strives to provide access to varied materials, services, and equipment for students, faculty, and staff and does not knowingly condone policies or practices that constitute an infringement of Federal copyright law. Transmitting or downloading any material that you do not have the right to make available and that infringes any patent, trademark, trade secret, copyright or other proprietary rights of any party is prohibited. Installing or distributing pirated or unlicensed software is also forbidden. Violation of these

requirements may subject students to *Student Handbook* violations, civil and criminal liabilities. Students who violate federal copyright law do so at their own risk.

Copyright status is applied to a work as soon as it is created. Users should assume that all writings and images are copyrighted.

Ross maintains a campus network to support and enhance the academic and administrative needs of our students, faculty, and staff. Ross is required by Federal Law to make an annual disclosure informing students that illegal distribution of copyrighted materials may lead to civil and/or criminal penalties. Ross takes steps to detect and punish users who illegally distribute copyrighted materials. Ross reserves the right to suspend or terminate network access to any campus user that violates this policy and Network access may be suspended if any use is impacting the operations of the network. Violations may be reported to appropriate authorities for criminal or civil prosecution. The existence and imposition of sanctions do not protect members of the campus community from any legal action by external entities.

Social Media Communications – Best practices

With the rise of new media and next-generation communications tools, the way in which Ross University communicates internally and externally continues to evolve. While this creates new opportunities for communications and collaboration, it also creates new responsibilities for everyone. The University recognizes its population is very diverse and that students, staff, and faculty may work or take classes in different locations. Staying connected with one's peers can be beneficial both academically and socially, and greatly contribute to student success. That connection may be in person, by email, phone, or instant messaging, or through social networks on the Internet that include but are not limited to Facebook® and MySpace®.

Ross University's intent of having a presence in the social media sphere is to facilitate connections between its audiences that participate in relational communication and to enable rapid response messaging in these emerging platforms; however, as this is a new platform for Ross University, it must ensure that all postings and usage adhere to Ross policies and approved content protect the integrity of the University, and maintain the trust of its key constituents. As such, Ross University retains the sole right to approve and publish all web pages containing information about its educational programs, services, activities on its behalf, student body, recognized student organizations, and body of alumni.

Student Club/Group Web Pages

Student groups or individual student web pages on any social media platform, such as MySpace, YouTube, FaceBook, forums or blogs are not under Ross University's purview. Therefore, they may not be used to promote, voice an opinion of, or recruit for Ross University in any way. Students must adhere to the *Student Handbook* when they engage in social media and mention Ross University. What applies as appropriate conduct on-campus or in online course shells also applies to conduct on social media platforms.

Ross University's intellectual property, including its trademarks, copyrights, logos and brands, is the exclusive property of Ross University. It is not to appear on individual or student group web pages or be used by individuals to promote themselves or their ideas and activities without prior written approval. Student groups that utilize any Ross University intellectual property on their social media pages without prior written approval will be required to remove them immediately.

Your Responsibilities:

It is important that all students understand their responsibilities when using social media. Please remember that you can have no reasonable expectation of privacy in material that you choose to place online or enter or send through resources provided by Ross. Recognize that you are responsible for anything you write or present online, and you may be subject to legal or *Student Handbook* proceedings by Ross University and/or others (ie, other students, employees, and third parties) based on what you write or present online.

Responsible behavior is expected of all Ross students when they participate in or partake of social media or blogging. Students' communications, regardless of format, must abide by the *Student Handbook*. It is not the goal of the University to actively monitor all student communications; however, should the

University become aware of inappropriate behavior that may violate the *Student Handbook*, the behavior may be investigated and addressed per the University's disciplinary procedures outlined in the *Student Handbook*. Such behavior includes, but is not limited to, posting or communication of content that is obscene, defamatory, threatening, infringing of intellectual property rights, or otherwise illegal, inappropriate, or injurious.

General Rules of Social Media Engagement:

Emerging platforms for online collaboration are fundamentally changing the way we work, offering new ways to engage with students, prospective students, alumni, our local communities, and the world at large. It is a new model for interaction and we believe social media, including blogs, can help Ross University build connectivity with its students. To foster this communication in an appropriate way, Ross University expects all students to follow the following principles of social media engagement.

Be transparent. Your honesty – or dishonesty – will be quickly noticed in the social media environment. If you are blogging about your experiences here at Ross University, use your real name, identify your relationship with Ross University, and be clear about your role. If you have a vested interest in something you are discussing, be the first to point it out.

Be Judicious. Always use your best judgment and make sure your efforts are transparent by using the following rules for external speech relating to Ross:

- Ask permission to publish or report on conversations that are meant to be private or internal to Ross University, including conversations with individual students and Ross employees.
- All statements regarding Ross must be true and not misleading and all claims must be substantiated and approved.

Write what you know. Make sure you write and post about your areas of expertise, especially as related to Ross University and our degree programs. If you are writing about a topic with which Ross University is involved but about which you are not the Ross University expert, you should make this clear to your readers. Also, always write in the first person. If you publish to a website or blog outside of the control of Ross University, you must use the following disclaimer: *"The postings on this site are my own and don't necessarily represent Ross University's positions, strategies, or opinions."*

Think before you post

Students should keep in mind that what is written and posted in electronic formats on the Internet, instant messaging, email or social networks is easily accessible to all and will be in existence virtually forever. This means postings and other communications may be viewed by administrators of the University, potential employers, and scholarship boards. If there is something you would not want everyone to know about you, do not post it online.

Protect yourself

Personal information can be shared over the Internet with more people and at a faster rate than ever before; accordingly, be careful what you share. Protect your personal information to avoid being a victim of sexual assault, stalking, identity theft, or burglary.

Always use privacy settings on social networking websites and in instant messaging, and only add people you know personally. Remember, you are not the only one who can be whoever you want to be on the Internet.

Effective date and change management

Amended 3/4/2010 by Anton de Freitas, IT Operations and Compliance Administrator
Approved 3/4/2010 by Ron Spaide, VP and Chief Information Officer.