Electronic Information and Communication

Since technology is advancing so rapidly, this policy does not attempt to list each and every element of the College’s policy on electronic information and communication usage. Rather, it is merely a reference tool, outlining the College’s philosophy and general principles and prohibitions to be applied when using College-owned equipment. If you have any doubts on a particular issue or use, check with your supervisor first.

The telephone system, facsimile machines, voice mail system, electronic mail system (e-mail), computers, computer network system, the Internet, any other electronic communication system, and the equipment and data stored on these systems, the College’s “electronic information and communication systems” are College-owned property and remains so at all times. All messages and transmissions composed, sent, stored or received on the College’s electronic information and communication systems are and remain the exclusive property of the College and are not to be considered private property of any employee. As College-owned property, all messages on the College’s electronic information and communication systems are subject to disclosure to law enforcement or government officials, or to other parties through subpoena or its equivalent.

The College has invested significant time and money in its electronic information and communications systems for efficiency purposes and to better serve our customers. All employees are required to learn how to use the systems by reading the instructions or by asking management for assistance. All users of the College’s systems must comply with all software licenses, copyright and intellectual property laws, as well as all other state, federal or local laws.

The electronic information and communication systems of the College are to be used for business purposes only. If the systems are used for personal reasons, such communications on the systems shall be treated in the same manner as all other messages in accordance with this policy.

Employees cannot expect privacy rights to extend to the use of College-owned equipment or supplies. From time to time, such as when an employee is on vacation, a business trip or a leave of absence, when it is suspected that a College rule, regulation or policy is being violated, if it is suspected that College property is being used improperly, or simply to monitor system usage or job performance, a College representative may gain access to your voice mail or e-mail messages, your computer files, or any other College property to better serve our customers and for other business or legal needs. For these reasons, you should not expect messages left on
your voice mail, e-mail or other communication device to be private. In fact, you should consider this information accessible like any other shared business file.

Although employees have individual passwords, encryption keys or access codes to their voice mail, e-mail and computer network systems, communications created, stored, sent or retrieved on such systems are not confidential, as these systems are accessible at all times by the College. Even when a communication is erased or deleted, it is still stored and can be retrieved and reviewed. The College may review, audit, intercept, monitor, access, print and disclose all messages created, received, stored or sent over the College's information and communication systems, if and when business purposes require with or without notice.

Employees must comply with the College’s Password policy and may not use passwords or access codes that are unknown to management. All system passwords or access codes are the property of the College and must be available to management. Employees are restricted from using passwords or access codes of other employees to gain access to another employee’s e-mail, voice mail, or other stored communication without prior approval from the other employee or from a supervisor. Employees are prohibited from “hacking” into other systems or “cracking” other passwords or access codes. No electronic communication may be created, transmitted or stored which attempts to hide the true identity of the creator or sender.

Employees are prohibited from using the College’s information and communication systems in any way that may be deemed inappropriate, illegal, fraudulent, intimidating, disrupting or offensive to others, which includes, but is not limited to the transmission of sexually explicit messages and/or cartoons, offensive or vulgar language, ethnic or racial slurs, gender specific comments, or any other comment or message that offensively addresses someone’s age, religious or political beliefs, national origin, disability, veterans status, or anything else that may be construed as harassing, discriminating or disparaging to or of others. Users encountering or receiving such material should immediately report the incident to their supervisor. Use of the College’s information and communication systems in violation of a College policy, or that will damage the reputation of the College, or use for distributions, solicitations, advertisements or promotions whether for outside businesses, charitable, political, religious or other reasons) is prohibited. Users may not install software into their individual computers or the network without first receiving prior approval from management.

Employees are prohibited from disclosing any proprietary or confidential information of the College or another without first receiving approval from their supervisor. When authorized, employees are expected to exercise significant caution when transmitting proprietary and confidential information over an electronic communication system because of the abilities of others to “crack” the system. Any such message containing proprietary and confidential information should begin with a warning declaring that such information is confidential and proprietary to the College.

Employees are prohibited from recording a voice mail greeting or leaving an e-mail message that indicates that any message left on the system is confidential or private.

Inappropriate use of the College’s information and communication systems may result in disciplinary action, including but not limited to immediate termination. This policy applies to all employees of the College, or authorized users of the College’s systems.

SOCIAL MEDIA
Staff and faculty use of social media can pose risks to the College’s confidential and proprietary information, reputation, and brands, and can jeopardize the College’s compliance with business rules and laws. To minimize these business and legal risks, the College expects its staff and faculty to adhere to the following guidelines and rules regarding use of social media on any devise. If the College’s computer or other device is used to access social media, the College’s electronic information and communication policy is also applicable.

This policy requires that:

- Accounts established on behalf of WATC should be clearly stated and officially approved by the Vice President of Marketing, Recruiting, and Advancement.
- Each social media account will have designated official administrators.
- Inappropriate, offensive, injurious and illegal content may be removed by WATC employees identified as account administrators.

Social media is never to be used in a way that violates College policy or staff/faculty obligations. If a post would violate any College policy in another forum, it will also violate it in an online forum. Staff and faculty are prohibited from using social media to post or display comments about co-workers, students, and supervisors that are vulgar, obscene, threatening, intimidating, harassing, or a violation of the College’s workplace policies against discrimination, harassment, or hostility on account of age, race, religion, sex, ethnicity, nationality, disability, or other factors prohibited by law.

Staff and faculty of the College are prohibited from representing the views of the College in the social media unless they are assigned by management to do so as part of their job.

Since technology is advancing so rapidly, this policy does not attempt to list each and every element of the College’s policy on use of social media. Employees uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until discussed with your Dean or Director.

Inappropriate use of social media may result in disciplinary action, up to and including termination of employment.