Acceptable Usage Policy

Code for Ethical Use of Computing Resources

All members of the Becker community make use of technology in pursuing their primary academic and administrative endeavors at the College. Using the College's technology resources for incidental purposes is also permitted, but all usage use must comply with state and federal laws, as well as with Becker's own policies governing appropriate use of technology. Becker requires that technology resources are not 1) used in a way that consumes excessive network resources; 2) abused or wasted; 3) employed in a way that interferes with, damages or harms a person; 4) employed in a way that intentionally interferes with the business operations of the College or any other company; 5) used for commercial gain; 6) used for dishonest or personal advantage; or 7) used to publicly convey what would reasonably be considered a private matter concerning another employee or student. Computing resources may not be used to promote or facilitate illegal or inappropriate activities or to facilitate actions that violate academic integrity (these may include, but are not limited to, harassment, theft, DoS attacks, hacking, child pornography, sending or receiving pornographic images, selling papers or other course work, or copyright violation (including the distribution and reception of copyright protected music, movies and games which are obtained illegally). Please be aware that Becker will cooperate with internal and external authorities in the investigation of illegal activities. Becker is also obligated to report any instances of child pornography to the appropriate authorities.

Becker has a legitimate interest in protecting its investment in technology. Toward this end, the College reserves the right to require the registration of all technology-related devices used on campus, regardless of whether the device is owned by the institution or an individual; to prevent or restrict the use of technology brought on campus by faculty, staff and students; to identify and quarantine devices suspected of adversely affecting the network; to employ tools to monitor (at the port level) network-related activity, including bandwidth consumption and point-to-point file transfers; to monitor bandwidth consumption and restrict or eliminate bandwidth allocation to specific devices; to monitor the transmission and storage of confidential information; and to terminate without notice individual network and Internet access upon detecting activities that violate the law or College policies.

Certain kinds of computer abuse and computer-related fraud are not only prohibited by this policy, but are illegal and punishable by any or all of the following: civil sanctions, criminal fines or imprisonment.

Copies of Fraud and Related Activity in Connection with Computers (18 U.S.C. ÂÂ§ 1030) and the Wiretap and Electronic Communications Privacy Acts (18 U.S.C. ÂÂ§ÂÂ§ 2510-2520, 2701, 2710) are available from Becker's Human Resources Department or the Computing Services Desk. The College may report suspected illegal conduct to the appropriate authorities.

Limitations on Use of Computing Resources

Individual Access

All members of the community are obliged to act responsibly in the use of technology. Faculty, staff and students are expected to provide and maintain accurate data about themselves (i.e. date of birth, address, Social Security number, etc.) when updating personal information on any of Becker's administrative and academic systems.

An individual may access only those accounts, files, software, and other computing resources authorized under his or her particular username and password and for which a legal license exists. Individuals must take reasonable precautions to protect his or her account(s) information, including passwords, usernames and PINs. Sharing individual IDs and passwords is expressly prohibited. All members of the Becker community are expected to exercise care in logging out of network resources and applications, in regularly changing their individual password(s), and in maintaining the confidentiality of their password. It is also a violation of Massachusetts law to access a password protected file without proper authorization.

An individual who intentionally shares their user ID and password with another person, where the primary intent is to provide access where it would otherwise be unavailable, may be subject to disciplinary action up to and including expulsion and immediate termination.

Hacking

Hacking is the intentional, unauthorized access to hardware or software. A hacker is a person who breaks into computers, usually by gaining access to administrative controls, with the intent to take over, read, modify, or cause damage. With the exception of specific course-based activities designed to educate students which are conducted under specific faculty direction, Becker will not tolerate hacking or DoS attacks by students, employees, contractors, consultants, volunteers, visitors, or any other person or device. Responsible parties include those who instigate, plan, initiate, participate in, or perform hacking offenses.

Students, employees, volunteers, consultants and contractors suspected of engaging in hacking are expected to cooperate fully with Becker and legal authorities in the investigation of such incidents. In investigating complaints of possible violation of College policy, Becker reserves the right to examine the contents of personal computers used by faculty, staff and students or other computers attached to our network, without prior consent or knowledge of the individual being investigated. Becker also reserves the right to confiscate computers used by faculty, staff and students. Cooperation may include, but is not limited to, providing transaction logs, copies of electronic mail messages, data files, usage records, hardware, account and password information, or other information as required by those authorities. Those who are financially responsible for the perpetrators, such as parents or guardians, may also be held accountable.

Permission to Record

Faculty, staff and students may not use any technology resources on campus, especially those available on personal devices, to record conversations, lectures, or classroom interactions without the express consent of those individuals being recorded. Such actions may also violate state and federal law. Faculty, at their sole discretion, may elect to make their lectures available for recording. Members of the Becker community who intentionally record other students, faculty and staff without their prior written consent may form the basis of a civil libel action and may be subject to disciplinary action up to and including immediate termination and expulsion.

File Sharing Applications and Copyright Law

Person-to-person (P2P) applications allow individuals to electronically exchange music, movies, videos, software, games, books, text materials, images and other kinds of copyright-protected and non-copyright-protected information. While some owners of music, movies, books, images and software explicitly allow their products to be copied, many do not. It is best to assume that these materials are copyright protected, unless explicitly stated otherwise. Downloading and making available to other individuals copyrighted material, such as music, movies, videos, books, text, images and software, without permission of the rightful owner, violates the United States Copyright Act (Title 17, United States Code), which has significant potential liability for damages. Moreover, using P2P file sharing applications may contribute to an excessive consumption of bandwidth and create a potential security risk, which also violates Becker policy.

As part of Becker's efforts to comply with copyright law, Becker's Digital Millennium Copyright Act (DMCA) Policy can be viewed on the Becker's Web Site. This policy outlines the specific procedures that Becker will take if the College receives any copyright infringement notices.

Violations of copyright law may result in temporary or permanent loss of access rights, fines, assignment of financial responsibility, disciplinary action up to and including immediate termination of employment, expulsion as a student, and legal action.

Social Media

Becker is committed to maintaining an environment in which opposing views on issues of the day may be fully and freely aired. Such an environment requires all community members to tolerate expressions of opinion that differ from their own and that, in some instances, some people may find unpalatable; however, activities that violate the College's policy against harassment, or that constitute an invasion of another's privacy, do not promote free expression and undermine the environment that the College seeks to maintain. They also may result in the imposition of sanctions for violation of College policy. Additionally, untrue statements of fact that harm another's reputation may be defamatory and may subject the individual making such statements to civil action by the person harmed by such statements.

In addition, it is a violation to use official college logos or seals on social networking sites without prior authorization from the Office of Marketing and Strategic Communications. For more information, please review the Becker College Social Media Procedure guide.

Employees and students who choose to engage in blogs, chat rooms, discussion groups, Facebook, Twitter, bulletin boards or other forms of social media should do so with the understanding that they may inadvertently pose a threat to their own or others personal safety and personal privacy. Publishing personally identifiable content (i.e., photos, addresses, phone numbers, banking information, health information, etc.) can lead to identity theft, stalking and other potentially dangerous outcomes. Employees and students who engage in activities that compromise the privacy of others, or disclose or discuss confidential or proprietary information, are violating institutional policy and will be subject to appropriate sanctions.

Becker reminds students and employees who are acting in their individual capacity of their obligation to clearly state that opinions expressed are their own and not those of Becker College.

Electronic Mail Policy

E-mail is the communication medium of choice for the Becker community and the official vehicle by which the members of the College communicate with each other. Students, faculty and staff are all expected to read e-mail regularly to glean the critical information that is routinely conveyed.

Becker provides electronic mail services to the campus community, at the College's expense, in support of academic and administrative pursuits. Incidental personal use is also permitted, so long as the use does not violate federal or state laws, or College policy. Because employees may have access to sensitive information via e-mail, Becker prohibits the automatic forwarding of full-time employee e-mail accounts to third party e-mail accounts (such as Google, Yahoo, etc.). Over the past few years, phishing attacks via email have increased in number and impact. If any employee succumbs to a phishing attack that compromises email, his/her account will be temporality disabled until he/she takes a special Phishing training session.

These guidelines apply to electronic mail sent or stored on servers, on personal computers, on personal devices such as smartphones or tablets, and to all archived and backup e-mail files and folders created using Becker technology resources, regardless of where they reside. The College reserves the right to change these policies at any time as may be reasonable under the circumstance.

Use of Institutional and Assessment Data

All members of the Becker community make use of institutional and assessment data in pursing their academic and administrative endeavors at the College but all usage must comply with state and federal laws (e.g., HIPPA, FERPA, etc.), as well as with Becker's own policies governing appropriate use of institutional and assessment data. Becker requires that institutional and assessment data are not 1) employed in a way that interferes with, damages or harms a person; 2) employed in a way that intentionally interferes with the business operations of the College or any other company; 3) used for dishonest or personal advantage; 4) used to publically convey what would reasonably be considered private or confidential information concerning another employee, student, program, major, department, school, division, or the College; or 5) Information that, if disclosed to unauthorized

individuals, could have a significant impact on the College's legal or regulatory obligations or on its financial status, students, employees, or brand.

Use of Institutional Information

Information technology and data constitute valuable Becker assets. In order to protect the security, confidentiality and integrity of Becker data from unauthorized access, modification, disclosure, transmission or destruction, as well as to comply with applicable state and federal laws and regulations, all Becker data are now classified within security levels, with requirements on the usage of data at different levels. Employees are prohibited from access information of family members unless there is a specific business requirement for them to do so. In addition, only designated employees may request or handle student or employees social security numbers. If you are unsure of whether you have permission to handle social security numbers, please discuss this with your supervisor.

In addition, any employee or contractor that handles credit card information is subject to Becker's PCI Policy; employees or contractors that process certain types of financial information are also bound by Becker's Gramm-Leach-Bliley Policy.

Remote Access

In an effort to keep sensitive data secure, while also understanding that our changing culture requires work to be performed remotely, Becker employs Virtual Private Network (VPN) software to enable faculty, staff and a limited number of contractors to access certain technology resources remotely with appropriate approval. Faculty and staff are responsible for protecting confidential data and therefore should not downloaded confidential data to laptop computers or portable storage devices. VPN allows faculty and staff members to work with confidential data in a secure manner.

Blue Light Application

Becker has a mobile application called Becker BlueLight that is available to all students, faculty and staff which can be used to contact Campus Police and send your tracking information to Campus Police from your smart phone in the event of an emergency. This is an optional application. If you choose to use this application, it includes the following services:

- Location Tracking: Real time location tracking in an emergency situation and the ability to send this information to emergency contacts
- Text Alert: Sends text alerts to emergency contacts in an emergency situation

Promotional Photographs for Becker College

Becker reserves the right to take photos on the Becker campus and Becker public events and use those photos on the web and in print publications.

Policy Violations

Any person that violates any of the policies found in this Acceptable Usage Agreement will be subject to the same disciplinary actions as outlined in Becker's Confidentiality Agreement.

Last Revised on: 5/4/17