Acceptable Use Policy for Baker College Information Technology Resources

I. Introduction

This policy defines the accountability of all ("Users") as well as the boundaries of acceptable use of Baker College computing and communication resources. Baker College provides robust resources to support the information technology (IT) environment, including computers, data storage, mobile devices, electronic data, networks, software, email services, electronic information sources, voicemail, telephone services, and other products and services.

Baker College's computing and communication resources are the property of Baker College and are used to support the institutions Guiding Principles, including the advancement of education, services, community, and administrative business support services.

IT resources are provided for the use of faculty, staff, students, and courtesy affiliates. This policy is intended to help protect Baker College and its constituents as it relates to privacy and confidentiality as well as the overall integrity of Baker College IT resources. Having a sound and effective information technology environment is essential to the Mission and Guiding Principles of Baker College.

When utilizing Baker College resources, you agree to the Acceptable Use Policy for Baker College Information Technology Resources language.

II. Applicability

2.1 This Policy applies to all individuals using Baker College resources, regardless of affiliation (faculty, staff, students, and courtesy affiliates) or where the resources are accessed or used, i.e. Baker College campus or remote locations.

2.2 For usage within the Baker College campus IT environment, additional rules may apply to specific resources, including classrooms, business systems, networks, software, social media, databases, and other services and support. Rules will be consistent with this policy and could potentially enact additional requirements and/or responsibilities on the Users.

2.3 Access to Baker College resources may be wholly or partially restricted without prior notice and without consent.

2.4 Access to this Policy will be granted to Users through the website, handbook and/or catalog.

III. General Authorized Usage Overview

3.1 Baker College resources are provided for College-specific objectives, including supporting the College's mission, teaching, administrative actions, and student/student-life activities, including social media usage.

3.2 Users are granted access to Baker College IT resources and are responsible for all activity performed with their user IDs. Users should take appropriate precautions to ensure the security of their passwords and prevent others from obtaining access to their computer resources.

3.3 Inappropriate or supplementary use that inaccurately or inappropriately illustrates support or affiliation of products, services, or organizations, without written approval, is prohibited.

3.4 Usage of Baker College resources for supplementary personal use is done at the user's own risk. The College cannot and will not guarantee the continued operation, support, or security of IT resources.

3.5 Users are responsible for informing themselves of any Baker College policies or regulations that control the use of College resources prior to resource usage.

3.6 Users are expected to respect the privacy of other Users, including usage, content, or identities.

3.7 Users are required to comply with state, federal, and local laws as well as College policies. Additionally, Users are required to adhere to the rules and regulations dictated by third parties.

3.8 Users are expected to engage in safe and responsible security and computing practices in order to maintain the integrity of Baker College resources.

IV. Inappropriate Usage

4.1 The use of Baker College resources for private business, commercial activities, fund-raising, or advertising for non-College purposes is prohibited unless approved in advance.

4.2 Users must adhere to copyright, trade secret, patent, or other intellectual property or similar laws/regulations.

4.3 Using College resources for unlawful communications, including threats of violence, obscenity, child pornography, and harassing communication are prohibited and will immediately be reported to the local police department and/or campus safety.

4.4 Unauthorized access, modification, copies, or deletion of Users' accounts or resources, including files, is not allowed.

4.5 Users cannot use IT resources in a manner that impacts usage or activities of the resources by other Users including, but not limited to, the introduction of malicious software or malware.

4.6 Connecting unauthorized modems, routers, wireless access points, or other devices to Baker College resources is prohibited.

4.7 Interfering with the networking including, but not limited to, scanning, monitoring, intercepting, and altering network packets is expressly prohibited.

4.8 Baker College resources cannot be used to engage in patrician politics or promote/oppose ballot measures unless that use is approved by the President/CEO.

4.9 Users cannot access Baker College resources without the proper authority, which includes attempting to evade or circumvent user authentication and/or misrepresenting one's identity or affiliation.

V. Email and Electronic Communications

5.1 Access to Baker College email is a privilege that may be wholly or partially restricted without prior notice and without consent of the user.

5.2 An activity that may strain the email or network facilities is a violation of this policy. These activities include, but are not limited to, sending chain letter and widespread dissemination of unsolicited email.

5.3 Modification or forging of email information, including the header, is prohibited.

5.4 Confidentially of email or other electronic communication cannot be assured; therefore, Users should be aware of the risks when sending confidential, personal, financial, or sensitive information.

VI. Social Media

For specific policies, procedures, and code of conduct, please reference the following documents: *Baker College Student Social Media Code of Conduct and Baker College Faculty and Staff Social Media Policies and Procedures.*

VII. Privacy

7.1 Privacy is important to Baker College; however, Users should be aware that the data created or stored on Baker College resources remains the property of the College.

7.2 Users are expected to respect the privacy of other Users and not divulge personal data concerning faculty, staff, or students.

7.3 Authorized individuals of the Baker College IT environment will perform management tasks in a manner that fosters User trust.

7.4 The College does not routinely monitor individual usage; however, normal operations require the backup of data, logging of activities, monitoring general usage, logging files, and other similar activities. Baker College may access various resources in order to perform necessary maintenance, including security events.

VIII. Operational Security

8.1 The College may, without advanced notice to Users, take any action necessary to protect the interests of Baker College to ensure that the IT resources are stable and secure. Any action necessary will be taken including monitoring and scanning College resources.

8.2 Third-party intrusions, viruses, and physical access can compromise computing and communication security. Baker College takes reasonable precautions to minimize risks. Users must notify and report incidents to abuse@baker.edu .

8.3 Known or suspected violations of the *Acceptable Use Policy* or *Social Media Policies* should be reported immediate to abuse@baker.edu .

IV. Enforcement

9.1 Use of Baker College resources is a privilege and not a right. User's access to Baker College IT resources may be limited, suspended, or terminated if that User violates the Policy. The CIO or the Director of Security will address alleged violations of this Policy.

9.2 In addition to review of alleged violation of this Policy, the College may be obligated to report incidents to law enforcement.

9.3 Users who violate this Policy, other College policies, or external laws will be subject to disciplinary action and/or penalties.

9.4 If the CIO determines that a User has violated this Policy and determines that access should be limited or suspended, the User may appeal that decision to the System Executive Committee.

Definition:
Users: any authorized individual, including faculty, staff, students, or courtesy affiliate.

Policy History:

Revision History:
Adopted: May 2014
Adopted: April 2010