

# Acceptable Use Policy

The Sage Colleges strives to provide information technology resources to support teaching, learning, research and administrative functions. Access to these services is a privilege, not a right, and all members of the Sage community are expected to use these resources responsibly and to respect the rights of other users. The Information Technology services offered may vary over time as institutional priorities change or new technologies become available.

## Terms Used in this Document

Computing systems/services: all servers, network devices, telephones/voice mail, desktop computers and peripheral devices including, but not limited to printers, scanners, cameras, and projectors. Examples of computing systems include the Sage servers, network hubs, switches and routers, the Colleague databases (and information residing therein), computer labs, desktops in offices, and network access, including connection to the Internet.

*User: Any individual accessing the computing systems/services*

**Systems Administrators:** Include the Network Administrators, Colleague Database Administrators, MyPortal Site Administrator, MyPortal Content Administrators and Information Technology personnel authorized to provide backup systems support. Access to various modules of the Colleague system is regulated by the module leaders.

**Authorization:** Authorization may be granted by Systems Administrators or others who are responsible for the various systems/services and information provided to users.

## Purpose of this Document

Information technology at The Sage Colleges is intended to support teaching, learning, research and administrative functions of the College. This document outlines acceptable use of these resources and is intended to support the following:

- the reliability, availability and integrity of computing systems/services at The Sage Colleges
- the use of computing systems/services that is consistent with the use of other college facilities
- that rules governing their use are consistent with others outlined in student and employee handbooks
- processes for dealing with violations that are consistent with other such institutional processes

## Scope

This document applies to all users of The Sage Colleges computing systems/services, including faculty, students, staff, administrators and friends of the College. The policies outlined below apply to all systems operated by the College, whether administered institutionally or locally (within a division, office, club or other campus group). Also included are personally owned computers connected to the Colleges computing systems/services.

## Appropriate Use

**General Statement:** The computing systems/services of The Sage Colleges are intended to support the teaching, learning, research and administrative functions of the College. While the College understands that computing systems/services may be used for personal activities, it is expected that personal use will not interfere with the delivery of services to the larger community.

All computers connected to the network are required to be registered with the college and have current anti-virus software and operating system patches installed. As new threats to network security/integrity are discovered, other requirements may be added. Registration for all employees is automatic. Students will be informed of registration procedures when they arrive.

**Authorization:** Access for all users is limited to authorized areas. All users have access to home directories on one of the College's file servers, electronic library resources, Internet access via network connection and wireless, e-mail accounts on Gmail and community tools on MyPortal.

Access to information in the administrative databases (Colleague) is determined based on job requirements and subject to approval by the module leader and, if outside the individual's functional area, the Vice President, Administration and Planning. Access to certain portions of the databases (for example Human Resources, Payroll) is limited to the System Administrators and staff responsible for that information.

Authorized access to other computing systems/services is determined by the individual responsible for that system/service or the information contained therein.

## Prohibitions:

The following activities are prohibited:

- Unauthorized access to or modification of files, systems, or services or attempts to violate the security of systems/services
- Use of peer-to-peer file sharing or other services to obtain and/or share copyrighted material such as music or videos
- Unauthorized use of another individual's identification and password, allowing another person use and/or access to one's account login ID or password, or disguising one's identity while using computing systems/services
- Use of systems/services that interferes with their primary purpose of supporting teaching, learning, research, and administrative functions. This includes, but is not limited to: spamming, sending of chain letters, disproportionate use of resources, or any action that creates excessive network traffic or system load
- Use of texting, chat, Facebook, e-mail, cell/smart phones or other disruptive devices or apps during classes.
- Use of computing systems/services to send, save or view offensive material. Messages stored and/or transmitted must not contain content that may be reasonably considered offensive. Offensive material includes, but is not limited to sexual comments, jokes or images, racial slurs, gender specific comments, or any jokes or images that would offend someone on the basis of his or her race, color, religion, marital status, gender identity, characteristics and expression, sexual orientation, national origin, age, physical or mental disability, veteran status, domestic violence victim status, genetic predisposition and carrier status, previous convictions or arrests as specified by law, as well as any other category protected by applicable federal, state and local laws.
- Commercial use of Sage systems/services. Use of Sage systems/services for any non-Sage commercial venture

- Use of Sage systems/services for transmittal of commercial solicitations, advertisements, or promotions.
- Use of computing systems/services that is in violation of State, Federal, or Local law. Examples of such violations include copyright infringement, unlicensed installation of software, distributing, receiving or transmitting child pornography, and terrorism.
- Use in violation of College policies as outlined in the Student Conduct Code and Employee Handbook.
- Use of computing systems/services that implies College endorsement of any political party or political initiative or religious affiliation.
- Unauthorized hosting of web sites or servers
- Intentional creation and/or distribution of malware or other damaging programs.
- Modification or upgrade of Sage-owned desktop equipment without notification to the Director of Information Technology or Vice President for Administration and Planning.
- Modification of computing equipment in the computer labs, libraries, classrooms or other publicly accessible locations, including smartcards, laptops and other devices. Prohibited modifications include, but are not limited to, re-configuration, physical modification, and/or installation of software, without authorization from the Director of Information Technology.
- Removal of Sage owned equipment from the premises without prior authorization from the Director of Information Technology or Vice President for Administration and Planning.
- Inappropriate use of information stored in the Colleague database or unauthorized disclosure of such information
- Provision of Sage e-mail addresses to outside vendors/organizations
- Additional prohibitions may be instituted at any time at the discretion of the College.

## **Software**

Particular care must be taken by all members of the community to ensure the lawful use of College software. Virtually all commercially-developed software is copyrighted, and the Colleges may use it only according to the terms of the license. In some cases, employees may install software for use at home for College business, but only when licenses indicate that such use is appropriate. Those who violate the license or copyright of institution-purchased software are answerable to the College and may also be legally liable to the licensor or copyright holder. Use of unauthorized or unlicensed software of any type on Sage computer equipment is strictly prohibited.

## **System Integrity**

The Colleges provide access through SageNet to electronic mail and Internet services and are committed to providing reliable, high quality services. The network is the property of The Sage Colleges and the Colleges reserve the right to routinely monitor network traffic to ensure system integrity. In cases where system integrity has been adversely affected or is at risk for any reason (for example, because users have not maintained updated security/anti-virus protection), the Colleges reserve the right to interrupt network access until issues can be addressed.

While the Colleges respect the individual privacy of all users, it is important to recognize that no network is entirely secure. No system/service should be considered a secure medium for the transmittal of information of a sensitive or confidential nature.

The Sage Colleges value the privacy of individual users and users may expect that systems administrators and other college officials will not gain access to personal files, e-mails or other information without prior authorization from the user. There are some circumstances, however, where obtaining prior authorization from the user is not required. Those circumstances include:

- When there are reasonable grounds to believe that an individual is in violation of law or has breached College policy (as outlined in the Employee Handbook, Student Conduct Code or other official document of the College) and access or monitoring may produce evidence to support this allegation
- When needed to perform system maintenance, identify or diagnose system or network problems, identify security violations or vulnerabilities, or otherwise ensure that systems/services have not been jeopardized
- When required by law or to preserve public health and safety

Access without the consent of the user requires approval of the appropriate senior officer (Vice President for Student Life for students, Provost for faculty, supervising senior officers for staff/administrators in other areas), except when emergency access is needed to preserve system integrity. All such instances of access will be logged by the systems administrator and a record of all occurrences will be maintained by the Vice President for Administration and Planning.

## **Privacy of Student Records**

The policy on privacy of student records is articulated in the Student Handbook and in Appendix 4 of The Sage Colleges Employee Handbook.

## **Violations**

Suspected violations should be reported to the Vice President for Administration and Planning.

## **Students**

Violations will be handled in accordance with the Student Conduct Code. The Sage Colleges may notify appropriate police agencies if a violation involves illegal activity as defined by local, state or federal law.

## **Faculty, Staff and Administrators**

As indicated in Section 3.7 of The Sage Colleges Employee Handbook: "All employees are expected to perform their work for The Sage Colleges in a professional, ethical and responsible manner. Violation of College policies and offensive behavior in the workplace may be grounds for disciplinary action, up to and including termination of employment." The Sage Colleges may notify appropriate police agencies if a violation involves illegal activity as defined by local, state or federal law.

## **Other Account Holders**

Violations will result in loss of account privileges. The Sage Colleges may notify appropriate police agencies if a violation involves illegal activity as defined by local, state or federal law.

## **Related articles**

- [IT Strategic Plan](#) (IT Service Desk KB)
- [Self Service Applications](#) (IT Service Desk KB)
- [Review Process for Campus Technology Projects](#) (IT Service Desk KB)
- [Knowledge Base](#) (IT Service Desk KB)
- [Software Location and Availability](#) (IT Service Desk KB)
- [Acceptable Use Policy](#) (IT Service Desk KB)
- [IT Information Hub](#) (IT Service Desk KB)
- [Software Discounts](#) (IT Service Desk KB)
- [Classroom Technology Overview](#) (IT Service Desk KB)
- [Network and Security Services](#) (IT Service Desk KB)
- [VPN Agreement and Access](#) (IT Service Desk KB)
- [Where can I view my personal leave time in SageAdvisor?](#) (IT Service Desk KB)
- [Printing & Copying](#) (IT Service Desk KB)
- [How do I register for classes?](#) (IT Service Desk KB)
- [Where is the IT Service Desk located?](#) (IT Service Desk KB)

This policy is mirrored:

- [MIS](#)