Siena College Computing Use Policy

I   **Purpose:**

The purpose of this policy is to define the scope of computing resources on campus and establish principles and practices in the use of those resources. Siena College's computing resources are essential components of our ability to provide an effective learning environment for our students, to facilitate the academic work of our faculty and to provide efficient and effective business functions to serve all of the Siena community. In order for the community and the college to function effectively, there must be in place some simple and straightforward principles and practices. This computing use policy and the statements it contains are an attempt to do that. The power and flexibility of computing resources, coupled with the rapid development of advanced uses of computing resources means that it is impossible to develop detailed policies and practices in all areas. Therefore, many of the statements in this policy are necessarily general. On the other hand some areas of computer usage are clearly restricted by law (i.e. copyright violations) and other uses can be readily identified (such as personal use during an employee's official work time). In such areas, the statements in this document are more precise.

II   **Scope:**

All users of the college's computing resources agree to abide by the principles and practices presented in this policy through the process of obtaining an account on any of the college's centralized computing facilities or by the use of any stand-alone computer owned or leased by the college or a privately owned computer when connected to the college computing resources. Notwithstanding the general guidelines set forth in this policy, the college reserves the right to terminate or suspend the computing privileges of any member of the Siena community at any time, with or without advance notice.

III   **Definitions:**

Siena College's computing resources include, but are not limited to, devices and software owned, leased or maintained by the college, such as: any computers, FRANet, workstations, servers (multiple user systems

such as Banner), audio/visual equipment, and printers. Extended computing resources include all software loaded on or accessible through the college network or through remote access to the college computing devices.

- "Users" are defined as anyone (guests, groups, organizations, departments, students, faculty, administrators, and staff) who use a computer on campus or accesses campus resources while off-campus.

- "Confidential" information includes all Personally Identifiable Information (PII), SS Number, Financial Data, Enrollment Data, Housing Data, Institutional Grant Information, Contracts, Board of Trustees Information, or other sensitive information of an individual associated with Siena College or of the Institution of Siena College.

- "Public Folders" are network folders that are available to the community of users logged into the network.   The folders and the contents are viewable by any user and are not secured.

- "H/W" refers to Computer Hardware.

- "S/W" refers to Computer Software.

  Throughout this policy, the College's Department of Information Technology Services is referred to as "ITS."

IV   **Policy Statement:**

Siena College provides computing resources for the academic, research, and administrative purposes of the college. Use of the resources for commercial purposes or for personal profit is forbidden. The only exception to this rule is for the writing and publication of scholarly works that may incidentally provide revenues to the author(s). Even such writing and publication of scholarly works will cease if it is found to have a negative impact on the effectiveness of the college system resources for other users.

Personal non-business use of the resources by employees during their scheduled working hours is forbidden. Use of the Siena computing resources for personal non-business uses is tolerated (when done during non-working hours for employees) only as long as the impact on system performance and the consumption of expendables is insubstantial (as determined by the individual's supervisor or by the ITS staff).

Individually Owned Equipment:

Faculty, staff and students may connect personally owned computers to the network only if they abide by the Personal PC Guidelines. ITS will not provide any technical support for problems with any computer not owned by the college, except as outlined below.

Specifically, Siena ITS mandates the following process and support:

Student Owned Equipment:

- Students must come to the Helpdesk for any H/W assistance;
- Students must sign a release form for any H/W or S/W advice or assistance (assuming the individual is not a minor);
- ITS will provide advice and guidance but will not perform any loading or unloading of software that could possibly put the college at risk or liable for any issues;
- In case of student owned equipment having negative effects on the Siena Network or causing issues then Siena reserves the right to remove the student's equipment from the network and the student should contact the ITS Helpdesk to seek guidance for resolving the problem prior to re-entering Siena's network environment.

Faculty and Staff owned equipment:

- ITS will not provide any H/W or S/W support for non-college owned equipment.
- Network access for computers is provided for academic and research purposes only, any non-business usage is not condoned and ITS may revoke the right of that individual to connect to the college network.

College owned equipment:

- ITS provides the H/W and S/W support for college owned equipment, and will setup the networking as required.
- ITS supports the "standard software" running on the equipment and the network connectivity to other computing, printing, and Internet resources.

Security

All users agree to assist Siena College in maintaining the integrity and security of its computer systems. System and network accounts are

issued to individual users or pre-established groups of users. Individual accounts are not to be used by any other user. Group accounts are not to be used by anyone outside the specified group. Users are responsible for any activity in their account, by anyone logged on to their account.

A. Data Security

The focus of data security is to protect data from corruption or unauthorized access, and to ensure privacy and confidentiality of personal and college data.

a) Custodian of Data/ Maintaining Confidentiality

Once an individual is granted access to data, s/he is responsible as a custodian of that data. Data custodians are held accountable for maintaining the security and confidentiality of those records to which they are granted access.

- Student Information **-** Faculty, administrators, staff, and student employees must comply with the college's policy under the Family Educational Rights and Privacy Act (FERPA) regarding the release of student information. (See *Siena Life* and the College Catalog).

- Non-student Information - Siena recognizes that non-student information is also essential to effective operations of the college and therefore will make such college data accessible to many employees.

- Use of data restricted to job responsibilities **-** Depending on the job responsibilities, information accessible to the user may range from the data of other employees, the financial records of individuals, departments, programs or the institution as a whole, to actual or potential donors, and other proprietary information.

- Responsibility to determine appropriateness of information release **-** In the event there is any doubt about the appropriateness of disclosure of information the employee should first consult his or her supervisor before releasing that information.

b) Request for System Access

In order to obtain access to Siena network, e-mail, and Banner systems, the user must submit an Account Request Form to the ITS Helpdesk. In the case of a new employee, the immediate supervisor must inform ITS that the new employee requires access to certain systems. Upon approval from the user's immediate supervisor or area VP, the user will be granted access to the system(s) and the appropriate data on the systems.

For part-time employee, temporary worker, and volunteers to obtain access to the systems the immediate supervisor or area VP must review the access requirements of the user with the ITS department, and when

agreed to the level of access and timeframe of the user, the requested access to the system(s) and the appropriate data on the systems will be granted.

c) Data Backup

This Data Backup policy is to protect and secure the data files (including but not limited to word processing documents and spreadsheets) that contain confidential information produced for the purpose of conducting the business of Siena College. These data files must be stored on networked storage devices that are regularly backed up by ITS, such as "My Documents" folder in the Sienaservices domain.
Business/Confidential data files may also be stored on the secure servers and applications that are authorized by the college. These confidential/business data files should not be stored on local hard drives, flash drives, or other devices that are vulnerable to being lost or stolen. ITS will provide adequate network storage for the custodians of those confidential/business data. It is the responsibility of the user to backup data files which are not stored on the allocated storage devices or the authorized hosted services.

d) Data Tampering

Reading, tampering with, deleting, or transferring any computer files or parts of files without the owner's express permission is unacceptable. Such actions may constitute theft or plagiarism.

Transferring any information legitimately obtained from or contained within Siena computing resources to an individual or group not authorized to possess that information is unacceptable and may constitute theft.

Unauthorized use of a computer and tampering with computers and computer-contained information, as determined by the college, are violations of one or more subsections of Section 156 of the New York State Penal Law. Such violations may be referred to appropriate police and law enforcement agencies and/or may be the subject of sanctions as set forth in Section regarding "Violations/Sanctions."

B. Account Passwords

Any computer or device that is connected to the college network, whether it is through a wired, wireless, VPN (virtual private network) or dialup connection must conform to the password requirements below. Any device or computer found in violation of these requirements risks being disconnected from the campus network.

All users are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

a) Requirements

- All network passwords (Siena.edu domain) are encouraged to be changed <u>on a regular basis, suggested as at least twice a year</u>. Previous passwords may not be reused.

- Passwords must not be inserted into email messages or other forms of electronic communications (without proper encryption).

- Passwords for all network and local computer accounts must conform to the guidelines described in the Password Policy. This includes ANY machine connected to the college's wired or wireless network.

- Anyone with a Siena account must use Strong Passwords (see Strong Password Guidelines in the Password Policy).

- Passwords should not be shared nor given to any other person.

b) Enforcement

Password integrity testing may be performed on a periodic or random basis by Siena College's ITS department or hired third party. If a password is determined to be insecure during one of these scans, the user will be required to change it. Anyone found to have violated this policy may be subject to disciplinary actions, which may include:

- Privileges being suspended

- Loss of access to network or systems resource

C. Computer Security

Personal computers require special security procedures. Any confidential information should be stored in a secure location. Confidential information stored in the following media should be password protected, zipped or encrypted.

- CD/DVD;
- USB Drives (thumb-drives or flash-drives);
- External hard-drives that are mobile;
- Any other removable media;

D. Public Folders

Siena College requires that no confidential information is stored in the Public Folders.

Laptop and Portable Electronic Devices

For information regarding Siena's **Laptop and Portable Electronic Devices Security Policy**, please go to ITS' Technology web site (siena.edu/technology) and click on the "Policies and Procedures" Section.

Software

Federal copyright law (17 U.S.C. §107 *et seq.)* recognizes that software is included in copyright protections. All software loaded onto any college computing resource must be legally obtained and legally installed (the installer or user must be able to demonstrate that they have a valid software license for all installations of that software or that the software is freeware). If no license is demonstrated within a reasonable period of time and there is reasonable basis to believe that the software has been illegally obtained, then the ITS staff will remove it.

Damaging, modifying, replacing, or copying any college-owned software (including operating systems) is not permitted due to the necessity of institutional standards for hardware and software. For a list of supported software, contact ITS or consult the college website. Game playing, other than simulation or other software utilized in courses or research, is not supported. Any data that is stored for leisure gaming usage, especially large data sets that are not used for academic or business purposes, will be removed.   Any games found on college equipment may be deleted by office supervisors or ITS staff.

a) Unacceptable software

In keeping with the college's position against harassment, any software that creates a hostile work or educational environment is not acceptable on any college computing resource. This would include such items as screen savers, wallpapers, posters, and audio clips, as well as any other software that could be deemed to have a sexual, racial, ethnic, homophobic, or other inappropriate theme. Such software will be removed by ITS staff whenever found on machines and is in violation of the Human Rights Policy.

Internet

The Internet connection is provided as a tool to assist Siena faculty, students, and staff in the educational, research, and business functions of the college. It is not provided for the personal non-business use of employees.

a) Illegal, Unethical and Unacceptable Material

No material will be published on any Siena websites that violates any licensing or contractual agreement, copyright law, college regulation or policy (FERPA, Campus Crime Security Act, etc.).

Members of the Siena community will be subject to disciplinary action for unauthorized P2P file sharing. Students will be sanctioned in accordance with the Student Code of Conduct in Siena Life. Faculty, Staff, and Administrators found in violation will be subject to varying sanctions, up to and including, termination of employment from the College. To ensure permissible downloading of music and the like, contact ITS for more information on File Sharing and Copyright.

All users of the Internet through the Siena College's computing resources must agree to refrain from any activity that is unethical and unacceptable. Activity that is unethical and unacceptable includes but is not limited to:

- Seeking to gain unauthorized access to the resources of the Internet,
- Disrupting the intended use of the Internet,
- Wasting resources (people, capacity, computer) through such actions,
- Destroying the integrity of computer based information,
- Compromising the privacy of users, without a legitimate college interest.

b) Intranet

The college reserves the right to designate certain materials, pages, and documents to be for internal use only. Information thus designated must be published to protected areas within the college's intranet that are not viewable to the general public.

c) Additional Utilities

The College Webmaster, reserves the right to deny or prohibit the use of additional internet utilities. An appeal to any decision can be made to the appropriate Vice President or to the Chief Information Officer.

World Wide Web

The "web" (also known as the "world wide web" or "www") allows institutions and individuals to create an electronic presence that may be viewed by anyone with appropriate software and internet access. Siena College has defined the Web Governance and Web Style Guidelines under the Web Advisory Committee (WAC).   The Governance model is separate from this Computing Use Policy and

is maintained by the WAC. This includes the Siena College website(s) and any content, tools, and materials associated with the web.

Social Networking/Online Communities' Websites for many, particularly students, are a powerful means for developing and strengthening peer connections and expressing individual identities through online communities (Facebook, Twitter, and the like). While the college does not officially monitor these types of websites, Departments (i.e., Student Affairs, Academic Affairs, and Human Resources) and Divisions of Schools may have specific policies concerning the user of social networking websites. Instances where a college official encounters a website reflecting inappropriate conduct by a member of the Siena community or inappropriate conduct brought to the attention of college officials, will be addressed through the existing response mechanisms at the College, including, but not limited to, the filing of a complaint under the college's Human Rights Policy or through the Code of Conduct Review process set forth in Siena Life.

E-Communications

For information regarding Siena's *E-Communications Policy* which covers E-Mail, please go to ITS' Technology web site (siena.edu/technology) and click on the "Policies and Procedures Section.

FRANet and Other Network Resources

A. FRANet

The FRANet system is designed to provide student access to Siena College's computing resources and the Internet using their personal computers in their residence halls. FRANet itself is a resource of the college and thus is regulated according to the responsible use policies and with consideration of the usage of the resources by the student community. In order to assure resource availability and prevent potential problems, the following rules must be observed:

- Users may not add hubs, web servers (including peer-to-peer file and music sharing software), game servers, ftp servers, or other hardware devices or software that may, in the judgment of ITS, put a strain on system resources, without first getting written consent from ITS.

- Users may not assign static IP addresses to their computers without the written consent of ITS.

- The uses of any unauthorized network tapping or "sniffer" devices or related software are prohibited.

- No copying and distribution of software, MP3 files, or other copyrighted material without the written consent of the copyright holder.

All student computers must be registered with ITS before gaining full access to FRANet. Unregistered computers will not be given access. Online game systems such as Xbox or PlayStation are allowed on FRANet. All gaming systems are required to be registered before being allowed access.

B. Other Network Resources

Disk quota - All users are assigned storage space on the college's network. Users who exceed their assigned amount of space will be asked to remove files. If the user does not comply after notification, ITS have the right to deny access to the network storage or, as a last resort, delete files. User may request help from ITS to manage their file storage space and/or attend a workshop to manage file system.

SienaAir - SienaAir is Siena College's wireless network. This connection is Internet only and can only be used to connect to sites available via the Internet. **Warning: there is no data encryption on this connection; therefore data is not secure. The college is providing access only to the Internet and does not take any responsibility for any personal information that may be intercepted by a third party through this connection.**

Users from outside the Siena community who use the SienaAir system are subject to the same restrictions on use as those who are Siena students, faculty, and staff.

Privacy

The college-owned computers and data stored on these computers are the property of Siena College [see the section on "Intellectual Property", which recognizes others' ownership rights, but does not limit the college's access to content on its computing resources]. The college also has the right to access the data stored and transmitted through its college-owned network. The college will endeavor to respect the privacy of the individual computer user. However, the college has the absolute right to examine the content stored in any medium through the college's computing resources for any reason deemed necessary to enforce its policies, comply with law and regulation, or otherwise further the legitimate and best interests of the college.

Intellectual Property

The provisions of the *Faculty Handbook* (Art. II, Sec. I. 1. "Patent and Copyright Policy") apply to all works composed, edited or transmitted using Siena College's computing resources. For the purposes of this document, the same terms are extended to the writing and publishing activities of Siena College's administration, staff and students.

This section of the handbook generally places ownership of original works with the creator of those works (except when created as part of specifically assigned job duties). This does not, however, preclude the college from accessing the files under the terms of the Section herein regarding "Privacy."

Freedom of Expression and Freedom of the Press

Contributing to, developing an individual or group home page or contributing to the Siena discussion board and other forms of electronic communications are tantamount to publishing. As such the freedom of expression applies as described in *Siena Life* or the appropriate College Handbook. At the same time, the freedom of the press has limits as described in *Siena Life* or the appropriate College Handbook. Among these limits are the requirements for accuracy, integrity, and decency. Attacks on individual persons (as opposed to differences of opinion) are not acceptable.

Responsibility for Monitoring Usage

Students, faculty, staff and administrators should be attentive to any abuses of Siena College's computing resources and report those abuses to the appropriate office.

Violations/Sanctions

Violations of any of these policies carry sanctions which may include, but are not limited to, reprimand, temporary or permanent cancellation of computer use accounts and privileges, disciplinary probation, suspension, expulsion or termination of employment. Sanctions will be determined by the appropriate body or individual using the existing policies and practices of the college as described elsewhere (Human Rights Policy, Employee and Faculty handbooks, *Siena Life*, current Human Resources policies, etc.).

Computing Privileges During an Investigation

When a violation is alleged, the system administrator or other appropriate college official will inform the alleged violator that he or she must cooperate in the investigation or the alleged perpetrator's account will be closed. User account

privileges remain in effect until the investigation is complete, except in cases where there is need for immediate action to assure the safety of property or persons, where the alleged perpetrator refuses to cooperate with the investigation, or where there is reason to believe that the alleged perpetrator may destroy evidence.

Right to Modify Policy

The college reserves the right to modify or change this policy in its absolute discretion.

IV **Governance:**

This policy will be updated by the Department of ITS. It will be approved by the CIO and President's Cabinet.

V **Exceptions:**

Exceptions can be granted in limited circumstances by the CIO based upon the needs of the college and upon the requestor's written justification, which has been reviewed and approved by the College's Risk Officer.

VI **Revision History:**

Date	Revision #	Modification	Approved Date
11/28/11	4.0	Cabinet Approval	11/28/11