Belmont Abbey College Computer and Network User Policy

I. Overview

Belmont Abbey College strives to maintain access for its faculty, administrators, staff, and students to local, national, and international sources of information and to provide an atmosphere that encourages the sharing of knowledge, the creative process and collaborative efforts within the College's educational, research, and public service programs.

Access to electronic information systems at Belmont Abbey College is a privilege which can be revoked, not a right, and must be treated as such by all users of these systems. With this privilege, come the following responsibilities:

- All users must act honestly and responsibly.
- Every user is responsible for the integrity of these information resources.
- All users must observe appropriate etiquette in electronic communication.
- Users are responsible for protecting their accounts from access by others, and shall keep private their passwords and ID's.
- All users must respect the rights of other computer users.
- All users must respect the integrity of the physical facilities and controls.
- All users must respect the pertinent license and contractual agreements related to College information systems.
- Users who incur access or user charges for services provided by off-campus services (such as commercial databases, processing time, etc.) are responsible for full payment of such charges.
- All users must act in accordance with relevant local, state, and federal laws and regulations.

Belmont Abbey College is a provider of a means to access the vast and growing amount of information available through electronic information resources. Belmont Abbey College is not a regulator of the content of that information and takes no responsibility for the content of information, except for that information the College itself, and those authorized to act on its behalf, create. Any person accessing information through Belmont Abbey College information systems must determine for him /herself whether any source is appropriate for viewing and use.

II. Scope of Policy

Any person accepting an account and/or using Belmont Abbey College's information systems shall constitute an agreement on behalf of the user to abide and be bound by the provisions of this policy. This includes any person using a privately-owned machine on the College's network. This also includes any person using the Internet service provided in the Residence Halls. Further, by this statement, the "Student Residence Hall Internet Use Agreement" is incorporated to this policy. This policy shall not impinge upon academic freedom with regards to research.

III. Definitions

"Campus Standard Hardware" shall mean brands and models of hardware that have been tested and found to be reliable and compatible with existing standards. All other hardware is non-standard. Examples of hardware include CPUs, external drives, input devices, network cards, modems, printers, etc. Please see the College's policy on Authority Guidelines and purchasing procedures. Network connectivity is assured for College-owned systems.

"Campus Standard Software" shall mean the College direction for particular types of software in campus-wide use have been tested and found to be reliable and compatible with existing standards. Examples of software include operating systems, networking software, and word processors.

"College" shall mean Belmont Abbey College.

"Electronic Communications" shall mean and include the use of information systems in the communicating or posting of information or material by way of social media, electronic mail, bulletin boards, World Wide Web (Internet), or other such electronic tools.

"Information Systems" shall mean and include computers, networks, servers, and other similar devices that are administered by the College and for which the College is responsible. It shall also include the high-speed Internet access system available in the Residence Halls.

"Networks" shall mean and include video, voice and data networks, routers, and storage devices.

"Obscene" with respect to obscene material shall mean:

- an average person applying contemporary community standards would find that the material taken as a whole predominantly appeals to the prurient interest or a shameful or morbid interest in nudity, sex, or excretion,
- the material taken as a whole lacks serious literary, artistic, political, or scientific value.

"Ponzi Scheme" shall mean a form of chain letter that requests recipients to send money or some other item of value to people on a list.

"Social Media" shall mean media designed to be disseminated through social interaction, created using highly accessible and scalable publishing techniques. Examples included but are not limited to Linkedin, Twitter, Facebook, YouTube, and MySpace.

"Users" shall mean all faculty, staff, students, associates, and guests with network accounts and/or access to the campus network and equipment.

IV. Restriction of Use

The College may restrict or prohibit the use of its information systems in response to complaints presenting evidence of violations of College policies and/or local, state or federal laws. Such complaints shall be addressed through established investigative and disciplinary procedures. Should it be determined that a violation has occurred, the College may restrict or prohibit access to its information systems, as well as any other disciplinary sanction deemed appropriate.

i. Permitted Use by Employees

College information systems are to be used predominantly for College-related business.

Limited personal use by employees is permitted as long as:

- It conforms to this policy.
- It does not interfere with College operations or performance of one's duties as an employee.
- It does not result in additional costs to the College.
- It does not require an inordinate amount of information systems resources (such as streaming audio and video for personal use).
- In the course of routine maintenance, should IT discover any violation of the above, IT staff is required to report to respective Vice President.

Information Technology does not collect and review data collected on network and internet use. When abuse appears from the top users, Information Technology shares the information about usage with the employee's supervisor. Action is taken only when directed.

ii. Obscene Material

College information systems may not be used to access, download, print, store, forward, transmit or distribute obscene material.

iii. Unauthorized Access

Unauthorized access to information systems is prohibited. This includes, but is not limited to:

- Use of another's password or ID.
- Trying to guess another's password of ID.
- Any attempt to circumvent system security.

When any user terminates his/her relationship with the College, his/her password and ID shall be denied further access to College computing resources.

V. Misuse of Information Services

Misuse of College an information service is prohibited and shall include, but not be limited to:

- Attempting to add, modify or remove computer equipment, software, or peripherals without proper authorization.
- Accessing without proper authorization computers, software, information or networks to which the College belongs, regardless of whether the resource accessed is owned by the College or the abuse takes place from a non-College site.
- Taking actions, without authorization, which interfere with the access of others to information systems.
- Circumventing, or attempting to circumvent, logon or other security measures.
- Using information systems for any illegal or unauthorized purpose.
- Personal use of information systems or electronic communications for non-College consulting, business or employment.
- Sending any fraudulent, harassing, threatening, discriminatory, or obscene electronic communication.
- Violating any individual software license or copyright, including copying, redistributing, or emailing copyrighted material, without the written authorization of the copyright owner.
- Using electronic communications to disclose proprietary information without the explicit permission of the owner.
- Using electronic communications to send chain letters or to initiate or perpetuate a Ponzi Scheme.
- Reading or accessing other users' information or files without permission.
- Academic dishonesty, including but not limited to plagiarism (see Student Handbook).
- Forging, fraudulently altering or falsifying, or otherwise misusing College or non-College records (including computerized records, permits, identification cards, or other documents or property).
- Using electronic communications to hoard, damage, or otherwise interfere with academic resources available electronically. This includes streaming audio and video for personal use.
- Launching a computer worm, computer virus, phishing, exploitive email, or other rogue program.
- Downloading or posting illegal, obscene, proprietary or damaging material to a College computer or network.
- Transporting illegal, obscene, proprietary or damaging material across a College network.
- Use of any College information system to access, download, print, store, forward, transmit, or distribute obscene material.
- Violating any local, state, or federal law or regulation in connection with use of any information system.
- Installing software not approved for use by the College on any College computer, network, or server.

- Modification or tampering of communication cabling.
- Unauthorized or obstruction of access to telecommunications closets.

VI. Use of Private Equipment

Use of privately-owned equipment is the responsibility of the owner of the equipment. The College will provide support for such equipment based on the standard support policies. Use of the College network is subject to all of the College policies herein.

The College is not responsible for any access to or damage of privately-owned equipment, its software, or its files connected to the College's network.

The owner is also responsible for any damage or compromise to the College's systems and/or equipment. Private equipment can only be connected to the Public/Wireless network or the Residential Network.

VII. Support Policies

There are multitudes of hardware and software choices on the market, and people naturally prefer to use those that suit their individual preferences. Many computer users rely on IT staff for training and support. It is impossible for the available staff to become experts on all hardware and software products. Therefore, hardware and software campus standards are necessary to make support activities as efficient as possible. Standards allow staff expertise and effort to concentrate on a limited set of essential applications and hardware systems that are widely used on campus. Concentration on standards allows support staff to build expertise in a manageable number of areas. It also focuses support services such as the Help Desk and training workshops to benefit the greatest number of users.

Standards also help users make decisions about hardware and software that are consistent with IT staff expertise and support programs. Standards, however, are not available for all possible applications that individual or departments may need to use. In addition, some users have needs for which the standard hardware or software is not ideal. In cases where non-standard hardware or software for desktop applications is selected, IT must limit the resources available to solve problems in order to meet our obligations for support of standards. Therefore, using non-standard products must assume a greater burden for self-reliance and independence. The following explains the support that IT will provide for various combinations of hardware and software.

Whenever standards have been set for hardware or software products, College policy requires purchase of the standard hardware and software be directed to Information Technology. There is no reimbursement provided for purchases outside of this process.

The College may announce the direction the campus will take for a particular application prior to the application becoming a standard. Support for the software will begin when the software is designated as a Campus Standard.

IT handles the replacement cycle for College-owned equipment and software. The current software and hardware standards will be applied. Functionality will be the same but the configuration may be different.

IT provides all standard computer hardware and software. Additional hardware and software may be purchased through IT.

VIII. Support Levels

Level 1 – Full Support (Provided for all Campus Standard hardware and software)

IT provides support (including Help Desk, troubleshooting, and when appropriate, training and documentation) for standard software and guarantees to the extent possible that the various standards will operate correctly together. IT will make every effort to get standard hardware or software working and bring in expertise as needed until the problem is solved or is found to be unsolvable. In such a case, IT will work to provide an alternate solution. However, if a software or hardware problem appears to be related to a conflict with non-standard or unapproved component(s), the component(s) will be removed.

Level 2 – Partial Support

IT support for Approved Software may include one or more of the following:
Making it work with standard hardware and software, making it available in our facilities, and basic training. For example, academic departments may wish to have software available in lab facilities for their students. In such cases, the professors are responsible for supporting the actual use of the program ("How do I use the quiz feature of the program?"), in conjunction with the manufacturer. IT support is limited to attempting to make the program run and print on the network.

IT will devote up to one hour attempting to connect non-standard College-owned hardware to the network. If the problem cannot be resolved during that time, IT will not research or refer the problem. IF campus standard network software and configuration settings or variations compatible with the network do not work, the hardware will not be connected to the network.

Level 3 – No Support (applies to software and hardware that is not standard or has not been approved for use on the campus network)

When time permits, a best-guess effort will be made to troubleshoot and correct problems that involve non-standard hardware and non-standard software. "Best guess" means that the IT Help Desk will suggest solutions or steps toward resolution of problems based on their expertise and experience. In such a case, there will be no research on the problem, office visits or referral

of the problem beyond the Help Desk for work by other IT staff. Users who purchase non-standard hardware and unsupported software assume an obligation for self-support. They should learn what support and assistance the vendor or manufacturer provides before making a decision to purchase. An example is the purchase of mobile devices and cell phones.

IX. Use of Computer Labs/Facilities

Users of computer labs are obligated to all policies herein and to any supplemental policies posted in that lab. Further regulations include but are not limited to:

- Food, drink (not in a closed container), or tobacco use is not permitted in computer labs.
- Priority of use and hours of use is as posted in the specific lab.
- Users must exercise proper care of the equipment in the lab.
- Users shall not attempt to remove, repair, reconfigure, move, modify or attach any external device to the computer(s) or system.
- Users shall not attempt to add, delete, or modify data, files, or programs.
- Users shall not attempt to circumvent security measures of the College or other users.
- Primary use of all labs is for academic and educational purposes. Users must be respectful of this in behavior.
- Users shall report any malfunction, concern, or violation of policy to IT.
- Users should avoid malware, phishing and other malicious software and sites.
- WARNING: computer and internet use is monitored and privileges can be revoked.

X. Privacy

When College information systems are functioning properly, a user can expect the files and data he/she generates to be private information, unless the creator of the file or data takes action to reveal it to others. However, users should be aware that no information system is 100% secure. Persons within and outside of the College may find ways to access files. ACCORDINGLY, THE **COLLEGE CANNOT AND DOES NOT GUARANTEE USER PRIVACY**, and users should be continuously aware of this fact.

Users should be aware that on occasion, duly authorized College information systems technological personnel have authority to access individual user fi8les or data in the process of performing repair or maintenance of computing equipment and systems. This may include the testing of systems in order to ensure adequate storage capacity and performance for College needs.

Information systems technology personnel performing repair or maintenance of computing equipment are prohibited by law from exceeding their authority of access for repair and maintenance purposes or from making any use of individual user files or data for any purpose other than repair or maintenance services performed by them.

XI. Electronic Communications (Email, Social Media, Telephones)

i. Email

Most inter-campus communication is transmitted via email; i.e., meeting notification, benefit information, campus events, etc. Employees and students are expected to check their emails periodically.

- Users should never assume that no one other than the addressee would read the message(s). Users should also be cautious about attachments and broad publication of messages. Copyright laws and license agreements also apply to email.
- Confidential or personal information; i.e., financial information, social security numbers, health records, etc. should never be sent via email. This information could be intercepted for fraudulent use. In this respect, blind copies should be sent with the utmost caution to ensure privacy. (Federal Red Flag Rule of 2010)
- The Federal Electronic Communications Privacy Act (ECPA) gives management the right to access and review all employee email messages transmitted or received via the College's computer system**. This policy serves as notification that administration may access and monitor email at any time for any reason without notice.**
- Emails must conform to the College's harassment and discrimination policies.
- Use of campus-wide email distribution lists is limited to College-related information and can be sent only by those persons approved to do so.
- Employees may not use the College email system to solicit for any purpose.
- Chain emails and/or graphics, which are not work-related, should not be forwarded. This type of email overloads the system and should be deleted.

ii. Social Media and Online Communities

Employee social networking during work hours is limited to those positions in which it is necessary to do so on behalf of the College and not personal. If you post on behalf of the College: acknowledge who you are, protect the institutional voice, and have a strategy for keeping information up-to-date.

Cyber communities and online social networking sites offer the opportunity to connect with peers online. It enables certain types of communication and connects likeminded individuals. However, actual experience has shown that the risks and negatives associated with these sites can far outweigh the positives. These risks and negatives are real for both the user and the College and include:

- Identity theft
- Cyber Stalking
- Damage to the reputation of individuals and the College
- Promotion of illegal, immoral, and College-prohibited behavior

- All College policies pertain to students' and employees' behavior even when they occur online. Therefore, someone that violates a College policy in an online community may face the same disciplinary sanction as someone that violates the same policy on campus.
- Sanctions for violation this policy will range from warning to dismissal from the College, depending upon the severity and/or repetition of the violation.
- Neither employees nor students are allowed to post images, photos, videos, or narratives online that show violations of the College's alcohol and drug policies, or other violations of College policies. Persons posting such images or are portrayed in this type of posting, may be found responsible for violating the College's alcohol and drug policies, as well as the College's policy on Defamation of the College Reputation.
- The College logo, pictures, videos, or stylized images of members of the College community cannot be posted without the written consent form the individual they represent. Any employee or student posting a picture, video, and/or stylized image of a member of the College community must remove the image immediately upon request. Failure to do so will result in disciplinary action.

Best Practices:

- Think twice before posting
- Strive for accuracy
- Be respectful
- Remember your audience
- Identify your view as your own

iii. Liability and Privacy

Electronic communications are an accepted and appropriate method of communicating. However, there are times when electronic communication is inappropriate. It may be more appropriate for a telephone call. The nature of the conversation should be the determining factor.

When using electronic communication you should be concerned with privacy and liability. Are you stating something which could have legal ramifications?

XII. Web Pages

All College web pages shall be designed in accordance with established regulations and guidelines as maintained by the Division of College Relations for the internet site. Intranet sites are maintained by Information Technology.

Creators of all web pages using College information systems shall comply with College policies and are responsible for complying with all local, state, and federal laws and regulations, including but not limited to: copyright, obscenity, libel, slander, and defamation laws.

Creators of a web page are responsible for the content of the page, including but not limited to accuracy of the information. Content should be reviewed on a timely basis to assure continued accuracy. Web pages should include contact information (phone number, address, or email) of the person to whom questions/comments should be addressed, as well as the most revision date.

XIII. Modification and Notification

This policy may be modified at any time in accordance with existing College practice and policy.

Notification of this policy and any modification shall be through established College channels of policy information.

Logging on to the College's network constitutes acceptance of the policies, procedures, and sanctions herein.

XIV. Application and Enforcement

This policy applies to all administrative and educational areas of the College. This policy applies to all employees and students of the College.

Enforcement of this policy shall be through normal enforcement of College policies.

Belmont Abbey College Computer and Network User Policy

Note: Keep the above copy of the "Belmont Abbey College Computer and Network User Policy" as a reference. Return signed page to the office that provided you this paperwork.

By affixing my signature below, I am acknowledging that I have read and understand the Belmont Abbey College Computer and Network Use Policy. I understand that access to the computer network at Belmont Abbey College is a privilege and if I fail to adhere to the regulations contained in the Computer Use Policy, my computer privileges may be revoked.

_____
Print Name

_____
Office/Department

_____
Signature

_____
Date