

IMMACULATA UNIVERSITY

ACCEPTABLE USE POLICY

Effective Date:

[Violations of this policy may be reported to abuse@immaculata.edu.]

- Authority** This Policy was approved by the President.
- Policy Statement** Users of the Immaculata University ("IU") network and computer resources have a responsibility to properly use and protect those information resources and to respect the rights of others. Use of IU computing, information technologies, and network resources is a privilege that depends upon appropriate use of those resources. Users who violate the law or IU policy regarding the use of computing resources, information technologies, and networks are subject to loss of access to those resources as well as to IU disciplinary and/or legal action as outlined in this policy.
- Policy Purpose** In support of academic instruction, research, public service, and administrative functions, IU encourages the use of, and provides access to, information technologies and network resources. Users of IU network and computer resources have a responsibility to protect those information resources and to respect the rights of others. This policy provides guidelines for the appropriate use of information technologies.
- Summary** Users of IU information resources must respect intellectual property, the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the rights of other information resource users. This policy covers the appropriate use of all information resources including computers, networks, and the information contained therein.

Section headings are:

1. POLICY SCOPE AND APPLICABILITY
2. OWNERSHIP
3. LIABILITY FOR LOSS OR DAMAGES
4. APPROPRIATE USE
5. INAPPROPRIATE USES
6. NO EXPECTATION OF PRIVACY
7. ENFORCEMENT
8. CONTACT

I. POLICY SCOPE AND APPLICABILITY

A. Applicability –

1. **“Users”** -- This policy applies to all IU employees, students, adjunct faculty, contractors, and volunteers who use computing resources, information technologies, networks, voice messaging equipment, computer software, data networking systems, including remote and wireless and electronically stored institutional data and messages owned or managed by IU or any third parties contracting with IU for the provision of hosting, network or other technology services (hereinafter **“Users”**). All such Users, by virtue of their use of IU computer resources, information technologies, and networks, accept the responsibility for using these resources only for appropriate IU activities. Users are responsible for reading, understanding, and behaving in a manner consistent with this policy and other related policies such as the IU Administrative Data Security Policy (if applicable) and the IU Copyright Policy.
2. **“IU Information Technology”** -- This policy governs the use of IU computing resources, information technologies, and networks. This includes, but is not limited to, computers, computing staff, hardware, software, networks, computing laboratories, databases, files, information, software licenses, computing-related contracts, network bandwidth, usernames, passwords, documentation, disks, CD-ROMs, DVDs, magnetic tapes, and other electronic media or storage devices (hereinafter **“IU Information Technology”**).

II. OWNERSHIP

IU retains absolute ownership of IU Information Technology. IU Information Technology are not owned by any individual or department at IU. Any IU Information Technology that are leased, licensed or purchased under research contracts or grants, must be administered under the terms of this policy and the IU Administrative Data Security Policy for as long as they remain within the lawful possession, custody and/or control of IU.

III. DISCLAIMER AND LIMITATION OF LIABILITY

IU makes no representations as to the performance, accuracy, or reliability of IU Information Technology. IU disclaims all warranties of any kind, expressed or implied, to the fullest extent permissible pursuant to applicable law, including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

By using IU Information Technology, you agree that IU, its trustees, faculty or employees shall have no liability whatsoever for damages in any form under any theory of liability or indemnity in connection with your use of IU Information Technology, even if IU has been advised of the possibility of such damages. You further recognize that IU

has no control over the content of information servers on external electronic systems or the Internet.

IV. APPROPRIATE USE OF IU INFORMATION TECHNOLOGY

IU Information Technology may be used for legitimate IU purposes only. While IU makes computer resources available primarily to achieve its goals of education and research, and for administrative activities, it realizes the need to encourage the personal use of computing for the convenience of the campus community. Thus, it is reasonable to allow the use of computing resources for email, document preparation, personal or course Web page publication, or other activity that can facilitate convenience or enhance productivity, to the extent that the activity is within the limits prescribed by this policy.

Appropriate uses of IU Information Technology include:

- Use by students related to completion of IU class assignments or their education at IU;
- Use by faculty, administrators, staff, and contractors directly related to instruction, research, and scholarly, professional, and administrative endeavors on behalf of IU or within the scope of IU employment;
- Appropriate use of resources (e.g. any such work is completed outside of university time and does not utilize shared resources such as CPU cycles or network bandwidth to a degree that adversely impacts academic or research activities);
- Appropriate use of licenses (e.g. do not use software procured with academic use licenses for commercial applications or development, unless the license explicitly permits such use).

If you are not clear on what constitutes an appropriate use, contact Thomas A. Egan, the Chief Information Officer of IU at tegan@immaculata.edu to determine whether a particular activity is permissible.

V. INAPPROPRIATE USES AND CONTENT

IU Information Technology shall not be used for:

A. Violating Intellectual Property Laws, Including:

- Violation copyright law pursuant to the IU Copyright Policy;
- Copying of software in violation of a license or when copying is not authorized;
- Violating trademark or patent law;

- Violations of any local, state or federal laws relating to intellectual property rights, such as the distribution of copyright-protected materials (e.g. the distribution of commercial software, music or films in electronic format without appropriate permissions by the owner, even if the user distributing the materials notifies others of their copyright status);

B. Any Prohibited Uses, Including:

- Supporting, establishing, or conducting any private business operation or commercial activity;
- Using any IU Information Technology, including a computer system, hardware (such as printers, monitors, etc) or networks without proper authorization or exceeding authorized use;
- Concealing your identity, or assuming the identity of another (e.g., by sending forged electronic mail). Keeping your identity private either by not setting an identity in your browser or by using a Web-anonymizer in order to protect yourself from being put onto mailing lists is not a violation of this policy;
- Unauthorized sharing of your password or account;
- Unauthorized use of IU Information Technology;
- Unauthorized use or attempted use of another person's computer account, userID, files, or data;
- Intentionally damaging, destroying or disrupting the electronic networks or information systems or the integrity of electronic information or intentionally wasting of human or electronic resources as they relate to IU Information Technology;
- Negligence leading to the damage of electronic information, computing/networking equipment and resources;
- Unauthorized use of a wireless router or other routing or electronic device that has not been authorized for use on an IU network or in conjunction with other IU Information Technology;
- Deleting or tampering with another User's files or with information stored by another User on any information-bearing medium (disk, tape, memory, etc.). Even if the User's files are unprotected, with the exception of files obviously intended for public reading, such as Web pages, it is improper for another User to read them unless the owner has given permission (e.g. in an announcement in class or on a computer bulletin board);
- Attempting to circumvent system security;

- Releasing programs such as viruses, Trojan horses, worms, etc., that disrupt other Users, damage any IU Information Technology, including software or hardware, disrupt network performance, or replicate themselves for malicious purpose;
- Sending mass mailings or commercial solicitations (i.e. spamming) to individuals, or to newsgroups or mailing lists where such advertising is not part of the purpose of the group or list or for the purpose of IU business;
- Harassing or intimidating another person (such as by repeatedly sending unwanted mail or broadcasting unsolicited mail);
- Tampering with, willful destruction of or theft of any IU Information Technology, including computer equipment, whether it belongs to IU or to an individual.;
- Violating IU's policy of prohibiting discrimination against individuals on the basis of race, sex (including sexual or other discriminatory harassment), religion, age, color, creed, national or ethnic origin, physical, mental, or sensory disability, marital status, sexual orientation, and status as a Vietnam-era or disabled Veteran;
- Intentionally disseminating, accessing, or providing a hyperlink to obscenity, as that term is defined by the law, unless such activities are directly related to a User's legitimate research or scholarship purpose or to completion of an academic requirement;
- Using IU Information Technology with the purpose of intentionally interfering with another User's use of IU Information Technology, such as computing resources, information technologies, or network resources;
- Unauthorized access to, interception, alteration, possession, copying or reading of electronic mail or other electronic documents or websites;
- Compromising the privacy of Users of IU Information Technology; and
- Violation of Any Federal, State or Local Law.

C. Any Prohibited Content, Including:

- Using IU Information Technology in any way that may be seen as insulting, disruptive, or offensive by other persons, or harmful to morale;
- Sending or distributing sexually explicit messages, cartoons, or jokes; unwelcome propositions of a sexual nature; ethnic or racial slurs; or any other message that can be construed to be harassment or disparagement of others based on their sex, race, disability, marital status, age, national origin,

religious or political beliefs or any other protected characteristic or status;

- o Accessing Internet pages which include offensive, sexually explicit and inappropriate material. Please note that even innocuous search requests may lead to sites with highly offensive content; and
- o Downloading non-academic related data or programs, including but not limited to freeware and shareware, such as:

- (a) Software that allows external access to any IU machine;
- (b) Peer-To-Peer (P2P) or similar software that enables content sharing;
- (c) Software that tracks user Internet or on-line activities or habits;
- (d) Software that sends information outside IU, unless expressly approved;
- (e) Software that sends automatic updates from the Internet to machines on the IU network;
- (f) Application programs (which may contain embedded viruses and/or may interfere with the functioning of standard PB applications); and
- (g) Downloading of music, video or any other material, in violation of copyright laws.

VI. NO EXPECTATION OF PRIVACY

Although IU does not routinely inspect or monitor use of computing and networking resources, IU does not guarantee the security and privacy of any User's electronic mail and/or electronic files. IU Information Technology are the property of IU and have been installed by IU to facilitate the legitimate purposes of IU. Although IU students, employees, faculty and others may have direct or password encoded access to IU Information Technology, they belong to IU and the contents of all communications and stored messages, including email, are accessible at all times by IU for legitimate purpose.

Your documents, files and electronic mail stored on an IU Information Technology are normally accessible only by you. However, system managers or third parties contracting with IU to host or manage IU Information Technology have the ability to monitor traffic and directly view any file as it moves across the network, and they must occasionally do so to manage campus network resources. In short, files may be monitored without notice in the ordinary course of business to ensure the smooth operation of the network. All administrative members, including staff, faculty, third party hosting providers and others working with IU Information Technology are obligated to follow the IU Administrative Data Security Policy, the IU Confidentiality of Student Records Policy (if applicable) and the IU Gramm Leach Bliley Act Required Information Security Policy (if applicable). Such policies create a framework for the physical, technical and administrative management, storage and transmission of data. These policies have clear guidelines that prohibit violations of privacy and confidentiality. You should be aware that authorized administrative personnel can and will take appropriate steps to investigate when there is a suspicion of inappropriate use of campus computing or

networking resources. This may include monitoring network traffic, its contents, and examining files on any computer system which is connected to the network.

You should also know that all files on shared (i.e., networked) systems, including email, are backed up periodically on schedules determined by IU. These back-up files can be used to restore files that were accidentally deleted. The maintenance, storage, access and transmission to such back-up files and data is operated in accordance with the IU Administrative Data Security Policy and the IU Gramm Leach Bliley Act Required Information Security Policy and/or agreements created pursuant to that policy that require the same level of physical, technical and administrative care.

Be informed that IU may access such electronic mail or files for a number of reasons, including but not limited to the following:

- A. Spam Blocking.** IU protects email as a viable communication and business medium by supporting measures to reduce the amount of unsolicited email Spam that invades its networks, while ensuring that legitimate email reaches its destination. To accomplish this task spam filtering software is utilized to quickly identify and separate spam from legitimate email.
- B. Requests for Public Disclosure.** The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) expands the authority of local, state and federal law enforcement to gain access to stored electronic data and communications. The USA PATRIOT Act is applicable to all Users.
- C. Retention of Electronic Mail.** Electronic mail is backed up and retained in accordance with IU data security policies. Be advised that even after erasing an electronic message from a hard drive, such materials continue to exist and may be subject to disclosure at a future time.
- D. Access for IU Business.** Faculty, staff and other administrators will only access a User's electronic files or email in accordance with the IU Confidentiality of Student Records Policy and IU Administrative Computing Security Policy. Any such access will be for a legitimate business purpose only and shall be limited to that purpose.
- E. Monitoring of Accounts.** An account may be inspected or monitored when:
 - 1. Activity from an account prevents access to IU Information Technology, such as computing or networking resources by others;
 - 2. General usage patterns indicate that an account is responsible for illegal activity;
 - 3. There are reports of violations of IU policy or any local, state or federal law;

4. It is necessary, in the judgment of IU administration, to do so to protect IU from liability;
5. IU receives a public records request or a valid subpoena; or
6. It is required by, and consistent with, any other law.

VII. USER'S RESPONSIBILITY FOR MAINTAINING PRIVACY

Users are responsible for maintaining appropriate access restrictions for their files, as well as protecting their passwords. Any User who knowingly allows another person to use his or her username or password may be found responsible for any inappropriate use on the part of that person.

VIII. ENFORCEMENT

Inappropriate behavior in the use of IU Information Technology is punishable under the general university policies and regulations regarding faculty, students and staff. The offenses mentioned in this policy range from relatively minor to extremely serious, though even a minor offense may be treated severely if it is repeated or malicious. Certain offenses may also be subject to prosecution under federal, state or local laws.

Appropriate disciplinary action depends not only on the nature of the offense, but also on the intent and previous history of the offender. The range of possible penalties includes reprimands, loss of computing privileges, course failures for students, disciplinary probation, suspension or dismissal from the university and/or criminal prosecution.

Offenses that are minor or appear to be accidental in nature are often handled in a very informal manner such as through electronic mail. More serious offenses will involve formal procedures pursued through the Division of Student Affairs for students, Human Resources and/or the hiring university department or administrative unit for staff, or the Faculty Review Committee for faculty.

Any User who suspects a violation of the IU Acceptable Use Policy or any other IU policy or regulation related to data security or who has knowledge of potential vulnerabilities or security loopholes in a system or network at IU, should immediately notify Dr. Thomas A. Egan, Chief Information Officer of IU (tegan@immaculata.edu), 12 Villa Maria * 1145 King Road, Immaculata, PA 19345, at 610-647-4400 x3868.

A. Restrictions of Privileges during Investigations

During the course of an investigation of alleged inappropriate or unauthorized use, it may be necessary to temporarily suspend a User's network or computing privileges, but only after determining there is at least a prima facie case against the individual, as well as a risk to IU Information Technology if privileges are not revoked. In these cases, it is important to recognize that the restriction of network or computing privileges is intended to protect the system rather than to punish the individual. For example, if a computer account has been used to

launch an attack on another system, that account will be rendered inactive until the investigation is complete. This is a necessary action taken to prevent further misuse and does not presume that the account holder initiated the misuse. Unsubstantiated reports of abuse will not result in the suspension of User account or network access unless sufficient evidence is provided to show that inappropriate activity occurred. For example, if someone reports that their computer was "attacked" by an account, the burden will be upon the complainant to provide sufficient data logs or other evidence to show that the incident did, indeed, at least appear to be an attack.

B. Adverse Impact on Shared Systems

IU reserves the right to discontinue communication with external systems that are known to harbor spammers or account crackers, despite the fact that this may restrict certain acceptable communications. When deemed necessary, this action will be taken to protect the security and safety of our systems. Similarly, there may be cases where a particular service or activity on a given IU system will, by the very nature of its legitimate operation, tend to generate attacks from other Internet sites. If these attacks are frequent and severe enough to cause service interruptions for larger parts of the campus community, it may be necessary to temporarily or permanently remove these systems from the campus network. In cases where such an action is deemed necessary, network administrators will work with the maintainers of the system to identify alternative methods of network access. In cases where IU restricts access to external sites or removes network access for internal sites, the purpose of the action is to maintain the security and reliability of the computer systems and networks rather than to punish an individual or a site, or to restrict the free expression of ideas.

IX. CONTACT

Questions concerning this policy or its intent should be directed to Dr. Thomas A. Egan, Chief Information Officer of IU (tegan@immaculata.edu), 12 Villa Maria * 1145 King Road, Immaculata, PA 19345, at 610-647-4400 x3868.