University of the Incarnate Word
POLICY ON THE ACCEPTABLE USE OF INFORMATION RESOURCES

Effective Date: October 3, 2007
Contact: Lisa Bazley, Vice President for Information Resources

INTRODUCTION

The University of the Incarnate Word provides a wide variety of technology resources to members of the university community. These resources are provided to empower students, faculty, and staff to learn and carry out the mission of the university. Protecting these resources and ensuring that they are readily available requires the participation and support of every member of this institution. It is the responsibility of every user of the university's technology resources to know these policies and use them appropriately.

Access to information resources at the University of the Incarnate Word is a privilege, not a right. This access is granted with restrictions and responsibilities for use. Violations of the rules governing the use of UIW information resources may subject the violator to loss of access privileges, disciplinary action, and/or other action as deemed appropriate by the university. UIW's information and computing resources are provided to support the university's academic, business, and research missions. Routine personal usage of these resources may be permissible if, in the determination of the university, such use does not interfere with the university's mission or preempt normal business/educational activity, does not impede employee productivity, does not interfere with or negatively impact any other person's or entity's rights and work/learning environment, does not conflict with any rule or law, and does not consume more than a trivial amount of resources.

PURPOSE

The purpose of this policy is to provide a high-level set of guidance regarding the use of information and computing resources at the University of the Incarnate Word. This policy is in place to ensure that users of university technology resources understand what is acceptable and unacceptable when using information resources provided by the institution. This policy is not, however, an all-inclusive list. Further guidance can be found in IRD standards and procedures, the Employee Handbook, the Faculty Handbook, and the Student Handbook. Guidance from these standards must be observed when using university information resources.

SCOPE

This policy applies to university faculty, staff, administrators, students, volunteers, contracted employees and other university affiliates privileged to use university information resources. In addition to this policy, all users of information and computing resources at UIW are also responsible for adherence to any State or Federal regulations regarding computer use at the university.

TERMS

Information and computing resources: Terms used interchangeably throughout this document, include but may not be limited to: email, file storage, electronic databases and other library information resources, software-as-a-service (SaaS) resources, electronic records, internet access, traditional computing devices, laptops, tablets, smart phones and the appropriate use of all

implemented systems, owned, licensed, or subscribed by the university. Guidance included in the Employee Handbook and the Student Handbook are incorporated by reference in this policy.

PROHIBITIONS

Account sharing is prohibited

The sharing of user accounts and/or passwords is strictly prohibited. Account owners are responsible for all activity conducted within their account. Failure to safeguard account information, or engaging in unauthorized account-sharing, may subject the account holder to disciplinary action.

Unauthorized access to network resources is prohibited

Attempting to access, alter, or remove any data without appropriate permission from the data owner is prohibited. The university reserves the right to access data and accounts as necessary to ensure the reliability and security of university information resources.

Commercial use prohibited

UIW information resources are provided for university operational and academic use only. Use of UIW resources for financial gain or commercial purposes is strictly prohibited.

Copyright violations are prohibited

Use of university information resources to share copyrighted materials (files, programs, songs, videos/movies, etc.) without permission of the copyright owner(s), is prohibited. Furthermore, the user may be in violation of copyright laws and the DMCA. When the Information Resources Division discovers or is informed of a copyright violation, Federal Law requires the removal of infringing materials immediately. If IRD is unable to remove these materials for any reason, then network access for the offending account or device will be terminated until removal of all infringing material is verified.

Identity theft or forgery is prohibited

Theft, forgery or other misrepresentation of identity via electronic or any other form of communication is prohibited. Suspected violations under State and Federal will be reported to appropriate authorities.

Physical modification to network resources is prohibited

Do not modify or extend network services and wiring beyond the area of their intended use. This applies to all network wiring, hardware, and jacks. Any student or employee performing unauthorized modification to or extension of network services may be held financially responsible for the cost of repairs.

Redirection or masking of services is prohibited

The UIW network may not be used to provide Internet access to anyone outside of the university community for any purposes. UIW-owned or commercially obtained network resources may not be retransmitted outside of the university community. Software or technology designed to hide internet usage (TOR, VPN, anonymizer proxies, etc.) is prohibited, unless a valid business or educational need is approved by the CIO.

Other prohibited activities

University information resources may not be used to:

- Operate a separate business or organization for profit or non-profit purposes.
- Monitor data on the network using monitoring or “sniffing” software.
- Provide a pass-through site to other campus hosts or provide remote login (e.g. telnet access) on your computer for others than yourself.

- Engage in any activities generally regarded or construed as "hacking."
- Harass, libel, or slander anyone or engage in fraudulent representations.
- Download, post, or transmit material contrary to UIW policies.

USER RESPONSIBILITIES

Preservation of resources

The university network is a shared resource, and users must respect others' need to use that resource. The university reserves the right to limit the use of individual computing resources at any time when necessary for the benefit of overall network operations or performance. Users or devices using unusually high bandwidth that affects the experience of other users may be disabled or speed-limited.

Prevent the spread of malware

The security of the UIW network is everyone's responsibility. Computers using the UIW network must include operational anti-virus software. Users must keep Virus Definition Files up to date. The university reserves the right to remove infected or vulnerable computers from the network.

No expectation of privacy

UIW makes every effort to respect the rights of network account holders. However, UIW reserves the right to monitor, intercept, block, or access data transmitted over the university network or, processed or stored on university resources as needed to ensure the reliability and security of UIW information resources. Therefore, we cannot and do not guarantee that users' e-mail or other network activity will be private, and users do not have an expectation of privacy.

EMAIL USAGE

Unauthorized Uses

Notwithstanding references made elsewhere in this policy to the personal use of UIW computing resources, UIW email account holders are not permitted to use UIW's e-mail resources for personal commercial or business activities, personal charitable endeavors, illegal political or other activities, to send or forward chain mail, or for any other purpose or activity prohibited by UIW policies or civil law, unless authorized in writing by the Vice President for Information Resources.

User Identity

Misrepresenting, obscuring, suppressing, or replacing a user's identity on an e-mail system is forbidden. The user name, e-mail address, organizational affiliation, and related information included with e-mail or postings must reflect the actual originator of the mail or postings.

Email etiquette

The university email system will be used in a professional manner, befitting a member of the university. Users will not engage in fraudulent, harassing, obscene, indecent, profane, intimidating, or unlawful communications using this system.

All users of the campus email system will ensure that communications are professional in tone and free of harassing language.

Stationary use, the use of personal "taglines" that quote a philosopher, religious text, use a "phrase of the day" or make any philosophical or political statement are prohibited, as are any image attachments as part of the sender's signature, except the university's official logo.

E-mail Purging and Archival

Emails will be retained in the university email system according to compliance requirements and

the business needs of the university.
Users may not "archive" email locally on their computers (i.e. in .pst files) and must instead use the archive function available in Office 365.
Users must move any email that they wish to keep beyond the automated retention period to the Office365 Archive folder.
The retention periods established by the Information Resources Department are defined in the IRD Email Retention and Management Standard.

Email Forwarding
Users are not authorized to auto-forward or otherwise automatically redirect their university email to accounts outside of the university mail system.

Use of Personal Email
University business may not be conducted using personal email accounts. The only authorized mechanism for conducting business is the university email system.

Duty to Protect
The security of university email resources is the responsibility of every user. Users will be cautious when clicking links in email or when sending information over the email system.

Personal Information
The university email system may not be used to transfer sensitive information. This includes, but is not limited to:

- Social Security Numbers
- Financial Information
- Health Information
- University Confidential Information

Inclusion of these information types in email may cause the system to reject the email.

WEB AND SOCIAL MEDIA

The UIW community has access to a variety of Web publishing options including personal and/or professional Web pages, weblogs or "blogs", course content pages, and departmental Web sites. Information on UIW's web site can be read worldwide. The quality, accuracy, and legality of this information are of the utmost concern to the university. The distributed and open nature of the Web renders traditional means of control impractical and transfers much of the responsibility to the individual. Students, faculty, and staff are responsible for the content of the documents they publish. They are also required to abide by all university policies regarding appropriate use of information and computing resources, including the following:

- Information, graphics, and other materials are covered by and subject to all current copyright laws. If permission to display text, graphics, sound, video, etc. that are owned by someone else has not been granted, do not publish it.
- If information about the university (e.g., total enrollment, number of faculty, etc.) is to be used, please confirm its accuracy. For assistance, please contact the Office of Communications and Marketing
- Information representing a point of view differing from an established university policy or position must comply with university publishing policies.
- All information must be free of inflammatory, derogatory, or offensive text, images, or sounds that exceed the bounds of academic freedom of faculty.
- Flaming behavior, as often seen in newsgroups, could be interpreted as libel, and should be avoided.

- The content of web pages, UIW discussion forums, blogs, and wikis are subject to all UIW policies.
- Every effort should be made to keep documents free of typographical and grammatical errors.
- Use of any UIW-sponsored web site for commercial and/or personal gain is prohibited.
- A phone number and/or e-mail address of the student, faculty, or staff member is to be included on the home page. The University of the Incarnate Word will not routinely monitor web page content, but we reserve the right to both monitor content and remove pages if they are in violation of these rules or relevant UIW policies.

ENFORCEMENT

Sanctions

Failure to comply with any of the above guidance or rules may result in termination of network services, loss of computing resource privileges, prosecution by the university, other disciplinary procedures, and/or civil and/or criminal prosecution. The Information Resources Division reserves the right to terminate any network connection without notice should it be determined that network traffic generated from said connection drastically inhibits or interferes with the use of the network by others. Depending on the circumstances, the university reserves the right not to indemnify you in the event of a claim or lawsuit by a third party related to the matters described in this policy.

Enforcement provisions

Violations of these rules are subject to the investigative and disciplinary procedures of the university with the appropriate representatives of the Information Resources Division acting in an advisory role. Complaints against students will be forwarded to and handled by the Director of Judicial Affairs. Complaints against faculty, staff and university affiliates are forwarded to and handled by the Office of Human Resources.

Limitations of privileges pending administrative or judicial process

In some cases, the university must act more immediately to protect its interests and resources, or the rights and safety of others. The Vice President of Information Resources (or his/her appointed representative) has the authority to suspend or limit account privileges and access to resources in those situations. When services have been suspended in this way, the Vice President for Information Resources shall notify the appropriate office, which will handle the complaint and attempt to notify the network account holder or computer owner. Account suspension, or removal from the network is typically temporary while the complaint is handled through the normal investigative and disciplinary procedures of the university.

Discipline for Violations

Failure to abide by this policy may result in disciplinary action, up to and including termination or being asked to leave the institution. The university investigates and responds to all reported concerns about the responsible use of information resources.

First Approved: October 3, 2007, version 1.0
Revised: October 1, 2008, version 1.1
Revised: June 14, 2013, version 1.2
Revised: February 28, 2018, version 2.0