COMPUTER USE

Hilbert College Computer Use Policy

I. Guiding Principles

Hilbert College's computing and network resources are to be used for College-related research, instruction, learning, and administrative activities. Unlawful or inappropriate use of these resources can be grounds for disciplinary action, legal action, or academic dismissal. The College expects faculty, staff, and students to use electronic resources in a lawful and responsible manner.

II. Conditions

Section 1. Hilbert College computer users shall use the college's computer and network facilities in a responsible manner consistent with the goals of the College.

- Hilbert College computer users shall use computer and network facilities in a manner consistent with all applicable Hilbert College handbooks and policies.
- Computer users are subject to all applicable federal, state, and local laws.
- Computer users who access external networks from Hilbert College will comply with the appropriate guidelines for use of those networks. Any personal use of Hilbert College computer and network services by Hilbert College employees shall not interfere with their official responsibilities and shall not violate any Hilbert College practice or policy.
- Use of Hilbert computing facilities for commercial, for-profit activities or for viewing or exchanging pornography is prohibited.
- Computer users shall not develop or intentionally spread viruses while using the Hilbert College computing facilities.
- Computer users shall not damage software or the computer hardware.
- Computer users shall not excessively waste paper.
- The College's network is a shared resource. Excessive or improper use of network resources that inhibit or interfere with the normal functioning of the network is strictly prohibited.

Section 2. Computer users shall access Hilbert computing facilities only with an authorized username and password.

- Hilbert College computer users shall not send electronic mail messages, print files on shared printers, or access off-campus computing facilities without being properly "logged in" with an authorized username assigned by the Hilbert College Information Services Department.
- Computer users should protect their passwords and not share their usernames and passwords with others.
- Computer users should also make sure that they are properly "logged out" of the computer when finished.
- Forgery, attempted forgery, spamming, or spoofing of electronic mail is prohibited.
- Computer users shall not falsify their network identity.

Section 3. Computer users shall respect the privacy of others.

- Computer users shall not intentionally read the information in anyone else's computer file(s), make copies of anyone else's computer file(s), write information back to anyone else's computer file(s), or engage in unauthorized transfer of file(s).
- Computer users shall not seek anyone else's passwords or modify anyone else's passwords.
- Hilbert College computer users shall not use electronic mail, Internet chat, or similar technologies as a means to harass, threaten, or send "hate mail" to others.

Section 4. Computer users shall respect the integrity of Hilbert College computing systems.

- The sharing of data on hard drives, or the operation of computer servers, gateways, hubs, switches, and routers by anyone other than authorized Hilbert College staff or faculty is strictly prohibited.
- Attempted to break-in to Hilbert College servers, attempts to gain access to Hilbert data, or de-facing of web pages is strictly prohibited.
- The use of "hacking tools" in an attempt to gain access to Hilbert's data is strictly prohibited.
- Computer users shall not send chain letters through electronic mail or spam e-mail.
- Hilbert College reserves the right to record and review any computer or network data for purposes of evaluating network performance, maintaining the College's computing environment, and the legal protection of the College.

Section 5. Computer users shall respect the legal protection provided by copyright and use licenses.

- Computer users shall not make copies of licensed Hilbert College computer programs to avoid paying appropriate license fees.
- Users shall respect all copyrights while using the Hilbert College network, Hilbert's software, and the Internet. This extends to the legal copyrights of music, video, or other materials that can be downloaded through the Internet.

Section 6. Peer-to-Peer File Sharing Policy.

- Unauthorized distribution of copyrighted material, such as through peer-to-peer networks, may subject students and/or employees to civil and criminal penalties.
- Copyright law protects the owners and creators of intellectual property from having their works stolen, copied, or distributed without permission. File sharing software that copies and distributes songs, movies, videos, games, and software applications without the permission of the owner can create both a criminal and civil liability for the user of the computer performing those actions. Content owners, such as the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) use technological means to track the file sharing of their intellectual property on the Internet.
- The college encourages the legal and authorized sharing of information and the free expression of ideas. Hilbert College also recognizes and respects intellectual property rights. Willfully taking, copying, or distributing other people's property without their permission or authorization is stealing and violates the college's standards for conduct. There is an obligation on the part of all those who use these campus facilities to respect the intellectual and access-rights of others who own or use the resources.
- All campus computer users (on any of Hilbert's networks) are warned to refrain from using peer-to-peer software applications to infringe on the distribution of copyrighted material. Note that many of these applications may scan your computer for other "legal copies" of music or movies and distribute those files automatically and without notice. Whether or not you have legally downloaded data, you are still responsible for the activities of your computer when connected to the campus network. Under federal rules and regulations, the college is obligated to educate, notify and inform all campus constituents of our policies regarding copyright infringement, P2P files sharing abuses, and the ramifications for violations.

6.1 Definitions

A. Copyright Act – the United States copyright law is written to protect the intellectual works of content creators. The law grants exclusive rights to creators of original works for a set period of time. There are volume's written on the role and formulation of copyright law, but for the purposes of this policy, if a piece of content (a song, a recording, a book, a movie, etc…) is copyrighted, it falls under the protection of this law. There are several exclusions for the use of copyright works in teaching, learning, research, fair use, library materials, etc… but for the most part this policy deals with the willful duplication and distribution of copyright materials without the owner's permission, in violation of copyright law.
B. Digital Millennium Copyright Act (DMCA) - the DMCA criminalizes certain actions used to violate copyright in the creation, distribution, dissemination, of protected materials. Most of the copyright enforcement over the past several years has been established under the provisions of the DMCA.
C. Recording Industry Association of America (RIAA) and Motion Picture Association of America (MPAA) – the RIAA and MPAA are trade groups that serve as agents for the content owned by their members. Many of the largest recording and movie companies are members of these associations. More recently these trade groups have taken on the duties to monitor and enforce the distribution, licensing, and royalties of the content owned by their members.
D. Peer-to-Peer (P2P) applications – software that is created to distribute and share digital material is generally referred to as P2P tools. While often used to bypass and circumvent copyright law, there are legitimate uses of P2P software as well. Over time, many of these software products have come under the attention of the various content owners and have either been removed from the marketplace, or in some cases the subject of lawsuits.
E. Take-down-notices, settlement letters, preservation letters, subpoenas – the courts and various content owners have taken numerous methods to reduce the illegal copying and distribution of copyright materials. A "take-down-notice" is the first communication that a content owner believes that their materials are being used in an illegal manner. The violator is notified to remove the offending content. Settlement letters have been used by the various trade groups to provide an opportunity to resolve a DMCA violation by the infringer paying a set amount to settle the complaint. Often a settlement letter to an individual is accompanied by a preservation letter to the college to collect evidence in network logs that would substantiate a legal claim of violation. The content owners may also pursue a violation through the courts and issue a subpoena to collect evidence of a violation.

6.2 Violation Notification

There are several ways that the college may become aware of a file sharing violation. The most common method is from network monitoring. The source is identified by the network IP address of the computer sharing the material on a specific date and time.

A. Network monitoring and identification of infringing activities – Information Service uses network based appliance to monitor and restrict activity. All know methods and techniques (including protocols) are currently blocked for illegal file sharing. In the event that we discover a new method or source, the offender is notified at once to cease activity and remove any copyrighted material. Information Services creates additional network policy rules to prevent further abuse.
B. Preserve Logs and Evidence – Information Services preserves the logs associated with the notification, identifying the computer/IP address/named user/location/date and time of the infringement.
C. Confirms Complaint – Information Services may scan or review the material in question to determine if it's likely that a violation/infringement has taken place.
D. Take Down Notice – Information Services reviews the complaint and begins an investigation to identify the computer/IP address/named user/location of the infringement.

6.3 Violation Response

Copyright infringement, P2P file sharing, and other network abuse infractions are handled through the regular campus disciplinary process. Depending on the identification of the computer in question, the incident may be handled by various departments:

A. Student - if a student computer is identified, the Office of Student Life is notified and the student disciplinary process is initiated.
B. Staff - if a staff member is identified, the Office of Human Resources is notified.
C. Faculty - if a faculty member is identified, the Office of Academic Affairs is notified.
D. Legal Counsel – there are many complex laws involved in the infringement of copyright, the actions on behalf of the content owners, the roles and responsibilities of network providers (such as the college), and the rights and responsibilities of individuals accused of violation. The college's legal counsel may become involved in these issues.
E. Forwarding Notices and Settlement Letters – conforming to all legal elements, the college will forward DMCA notices, take-down notices, and settlement letters to the individual as identified. How that individual responds to the complaint will be their responsibility.
F. Ramifications of policy violation – disciplinary actions for policy violations are intended to be redemptive and educational in the context of the college's mission. These actions can range from informing the person of their violation and letters that document the incident; to fines, penalties, loss of network privileges, suspension, expulsion, and termination of employment.

6.4 Alternative Services

The college currently permits downloads through iTunes and select other legal sources. The college will continue to evaluate legal alternative sources based on market demand and proven ability to uphold copyright standards.

Section 7. Expected Behavior in Hilbert College Computer Labs During Class.

- As a courtesy to fellow Computer Users and the instructor, Computer Users should avoid browsing the Internet, instant messaging, and other computer use that may prove disruptive to the instructor's presentations.
- The viewing of offensive or disruptive material during class is prohibited.

III. Additional conditions for resident computer users

Users of the Hilbert College Residence Hall Network are subject to the following conditions:

Hilbert College provides two computing environments within the Residence Facilities.

- **ResNet Wireless Network** – Internet Access for residents via the Hilbert ResNet Network for a nominal licensing fee. (See ResNet Application below)
- **Student Computer Lab** – A computer lab for residents is located in the Residence Hall. In addition to Internet access, this lab provides access to the Hilbert Intranet and various specialized computer applications used in the classroom.

RESNET Users:

- Only computers and wireless network adapters that have been registered with the Hilbert College Information Services Department may be used access the ResNet Wireless network. (See ResNet Application below)
- Computer Users may only access the network with a valid username and password.
- Computer Users may not use hubs, routers, wireless access points, or similar signal splitting devices to share ResNet services with unauthorized users. Connection to unauthorized network jacks or splicing of any kind is prohibited.
- Since the wireless network is designed to be a "shared" medium, computer users should exercise discretion when downloading large files from the Internet. Your actions affect your neighbors, and ultimately yourself.
- The Hilbert College Information Services Department shall have the sole authority to assign host names, network addresses, usernames, and passwords for computers attached to ResNet. Thus, users may not manually configure their computers to use network settings or network adapter cards other than the settings authorized.
- Hilbert College reserves the right to immediately disconnect any computer that is suspected of sending disruptive traffic to the network or causing problems on the network. This includes problems caused by defective cables, Ethernet cards, or other hardware/software problems. It will be the student's responsibility to correct any such problem before the computer will be allowed back on the ResNet network.

IV. Privacy Not Guaranteed on College Network

Information stored on the computer is normally treated by Information Technology Services as confidential and private. Nevertheless, computer users should be aware that privacy cannot be guaranteed in the case of legal or disciplinary proceedings. Computer users should be aware that information may appear on system backups, and even the deletion of messages or files may not eliminate information from the system. Claims of copyright infringement will result in removal of offending materials from Hilbert College computer systems under the Digital Millennium Copyright Act (DMCA). Where it appears that the integrity, security or functionality of the College's computer or network resources are at risk or in instances of abuse of College policies, standards, or local, state or federal laws, Hilbert College reserves the right to take whatever actions it deems necessary (including, but not limited to monitoring activity and viewing files) to investigate and resolve the situation. In such instances, a written report of the findings will be forwarded to the appropriate College officials. In order to assure continuity for academic and administrative departments, similar procedures may be used after an employee is separated from Hilbert or is no longer able to perform the required duties.

RESNET/WIRELESS USER INFORMATION

Resident Students:

Hilbert College provides Internet access via Wireless & Wired connections. To be connected, resident students are required to:

- Have a Hard Line or Wireless Adapter Card. For Hard Line/Wired a 10/100/1000 NIC Card, and for Wireless, a 802.11B/G/N compliant card.
- Only **Window XP, Windows Vista, and Macintosh OSX 10.4+** are supported.
- Hilbert Information Services will contact you with your access information.

Commuter Students:

Hilbert College provides commute students Internet access via Wireless ResNet. To be connected, commuter students are required to:

- Have a Laptop running **Window XP, Windows Vista, and Macintosh OSX 10.4+** with a 802.11B/G/N compliant card, and be registered with the Information Services department.