Intellectual Property

Copyright Law

Federal copyright law grants to the authors or creators of original works (books, plays, musical compositions, films, television programs, and many other kinds of works) the sole right to distribute, perform, display, or reproduce their work, to derive new works from their own original work, or to allow others to do any of the above. Published and unpublished works have equal protection. Copyright protection begins the moment a work is created, and works do not need to be registered with the U.S. Copyright Office to be protected.

The Fair Use provision of the federal copyright statute permits limited use of copyrighted material, without the author or creator's permission, for purposes that include teaching, scholarship, and research. Not all educational uses are considered fair use, however. The Digital Millennium Copyright Act (DMCA) of 1998, a significant update to federal copyright law, addresses the reality of copyright, and the additional threats to copyright holders, in the age of computer networks. The Technology, Education, and Copyright Harmonization Act (TEACH) rewrote a portion of the copyright statute to make it easier for universities to use copyrighted material in distance education and other activities that involve the electronic delivery of educational content to homes, businesses, and other off-campus sites.

WPI expects all members of its community to respect the rights of intellectual property owners by complying with copyright laws, and the university itself is committed to observing and enforcing these statutes. WPI also expects faculty, students, and staff who wish to take advantage of the Fair Use or TEACH Act provisions to familiarize themselves with those provisions and to make a good faith effort to determine whether permission is required before employing copyrighted material for any WPI-related use.

Faculty, students, and staff who deal with copyright issues on a regular basis are encouraged to take advantage of training programs on copyright issues offered from time to time by the staffs of Gordon Library and the Academic Technology Center.

WPI's Copyright Compliance:
www.wpi.edu/Pubs/Policies/Copyright

WPI recognizes that copyright law is complex; this site also provides background on copyright issues, with links to other sources of information.

Electronic Communications

Electronic Communications Privacy Act (ECPA)

The ECPA extended earlier wiretap statutes to protect various forms of electronic communications, including e-mail, network communications, and cell-phone calls, from surveillance by private, business, or government officials. The USA Patriot Act amended certain provisions of the ECPA, for example, by giving the federal government greater power to review e-mail stored on WPI's servers.

Be aware that WPI must comply with valid legal requests (e.g., court orders) to produce records of communications. Also, Network Operations will monitor network traffic to detect attacks, viruses, or excessive traffic, in order to continue to offer a high-performance network supporting the mission of WPI. There is no intention to monitor content of network traffic.

Given the "business extension exception" to the ECPA, it is valid for a supervisor to access e-mail of a subordinate for business purposes. At WPI, written direction of a division vice president can enable access to a subordinate's e-mail. However, please be aware that policies may be developed that might expand that access.

Computer Fraud and Abuse Act

This federal act makes it a crime to intrude on protected computer systems to obtain information or anything of value, to commit fraud, or to damage a computer. Protected systems are those used in interstate or foreign commerce or used by financial institutions and government agencies. Under the terms of WPI's Network Security Policy, the university's Network Operations and Security staff will report suspected intrusions to the appropriate authorities, including, depending on the circumstances, WPI's Police Department, and local, state and federal law enforcement officials, and will cooperate in the identification and prosecution of those who engage in network activities that violate WPI's policies and the law.

WPI's Acceptable Use Policy:
www.wpi.edu/Pubs/Policies/AUP

WPI's Network Security Policy:
www.wpi.edu/Pubs/Policies/netsec.html

The USA Patriot Act and WPI's Policy on Information Requests

All employees and student workers are encouraged to familiarize themselves with WPI's policy on information requests:
www.wpi.edu/Pubs/Policies/patriot.html

The USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), passed by Congress after the Sept. 11, 2001, terrorist attacks, gives federal law enforcement officials authority to access records and information that amends or supersedes provisions of two of the acts described in this brochure.

Specifically, the USA Patriot Act amends the Family Educational Rights and Privacy Act (FERPA) to permit or require educational institutions to disclose academic records to federal law enforcement officials without a student's consent or knowledge, in some circumstances. It also amends the Electronic Communications Privacy Act of 1986 (ECPA) to give the federal government greater power to review student and employee e-mail, among other provisions. [The USA Patriot Act also amends the Foreign Intelligence Surveillance Act of 1978 (FISA), which is not discussed in this brochure.]

Because of the complexity of the USA Patriot Act and the severity of penalties for educational institutions that violate its provisions, WPI has developed a policy that establishes an institutional protocol for responding to USA Patriot Act information requests. The protocol designates university officers who are authorized to respond to requests: Associate Treasurer, Associate Provost, Chief of Police, in that order; all other WPI employees must refer such requests to these officers.

The USA Patriot Act makes it a crime to notify an individual about whom information is sought. Therefore, anyone who receives an information request under the USA Patriot Act should discuss the request with no one, but should, instead, during regular business hours immediately contact the appropriate university officer. After regular business hours the person requesting the information should be told that the matter will be referred to an authorized officer during regular business hours.

2006–013

Information Security at WPI

An Overview for Employees and Students

WPI

2006-07

Information Security at WPI

An Overview for Employees and Students

WPI's telecommunications systems—its computers, servers, wired and wireless data networks, and phone system—are essential tools for conducting the day-to-day business of the university. Data processing, data storage, and electronic communications technology have made it possible for WPI to more effectively and efficiently perform such essential tasks as registering students for courses, recording their academic progress, and managing the complexities of WPI's financial data. In addition, it would be difficult to imagine students, educators, researchers, and administrators getting by today without the instant communication and access to information provided by e-mail, the Web, and network file transfers.

All technologies have risks as well as benefits. One of the greatest concerns about the use of systems that store and transmit information electronically is the increased risks that data will be intercepted, stolen, or corrupted; that confidential information will be inadvertently released to those who should not see it; and that individual rights (for example, the right to privacy, the right to remain free of harassment, and the right to control and profit from one's intellectual property) will be violated.

WPI takes seriously its obligation to operate its electronic data and communications systems in a secure manner and to carefully safeguard the personal and confidential data it maintains on students and employees. It has developed a host of policies and guidelines that outline procedures that should be followed by members of the WPI community to assure that the university lives up to that obligation.

A number of these policies respond directly to seven federal laws that deal with a wide range of legalities associated with information security. While this brochure focuses on electronic communications, it should be noted that these federal acts cover the dissemination of information in any form: orally, on paper, and through electronic means.

For a host of legal and financial reasons, it is critical that WPI comply fully with these seven acts. And because virtually all faculty, staff, and students are impacted by one or more of these laws on a daily basis and play important roles in assuring WPI's compliance, the university has prepared this brochure to familiarize you with the basic elements of these acts. You are encouraged to learn more about the acts and WPI's information security practices by following the Web links referenced below.

WPI offers a variety of training programs for faculty and staff whose work requires more than a general understanding of information security issues. Be sure to take advantage of progams that cover statutes that are relevant to your work.

Educational Records

Family Educational Rights and Privacy Act (FERPA)

WPI maintains a variety of educational records concerning its students. Official educational records are maintained by the Office of the Registrar; faculty and staff members may maintain unofficial records related to their academic work with students. FERPA details the rights of students to access their own official educational records and WPI's obligation to restrict others' access to them. The act covers three broad areas:

1. Access by Students: Students have the right to know what kinds of educational records WPI keeps, where they are kept, and for how long they are kept; they have the right to review and obtain copies of their own records (with some limitations); and they have the right to challenge the content of their records.

2. Disclosure by WPI: With limited exceptions, WPI may not release a student's educational records to anyone without the student's written consent. There is one important exception: records may be released without consent to school officials who have a legitimate educational interest in those records. WPI's FERPA Compliance Statement (see link at end of this section) explains who is considered a school official and what is considered a legitimate educational interest.

3. Directory Information: FERPA permits WPI to define certain items of student information as directory information and to release that data and publish it in an annual campus directory without students' consent. However, a student may request that his or her directory information not be released. This request must be submitted in writing to the Office of the Registrar by the end of the first week of classes in the fall (a "Request for Confidentiality" form may be found at wpi.edu/+registrar). WPI defines directory information as name, local and permanent addresses, e-mail address, class year, WPI mailbox number, local telephone number, major, and advisor.

What FERPA means for…

Students: As noted above, students have the right to prevent anyone except university employees with legitimate interest from accessing their academic records, the right to access their own records (with some limitations), and the right to challenge the content of those records. They also have the right to request that their directory information remain confidential.

Parents: Under FERPA, grades are considered academic records. It is WPI's current policy not to share grade reports or other academic records with parents or guardians of WPI students without the students' written consent.

Faculty: As part of the normal course of their work, members of the faculty receive and generate a host of academic information concerning their students. In addition, faculty members are frequently approached by third parties requesting information about students. It is, therefore, especially important that they be familiar with the provisions of FERPA and WPI's policies on student records, and take advantage of training programs offered by the registrar's office.

Staff: Especially in academic departments, staff members often receive requests for student information. Those who may be subject to such requests should review the policies below and take advantage of FERPA-related training programs offered by the registrar's office.

WPI's FERPA Compliance Statement:
www.wpi.edu/Admin/Registrar/ferpa.html

WPI's Student Records Privacy Guidelines:
www.wpi.edu/Pubs/Policies/ferpaguide.html

Health Records

Health Insurance Portability and Accountability Act (HIPAA)

WPI maintains a variety of medically related records for students and employees. Examples include receipts, claim forms, and other records related to employee health insurance claims or requests for reimbursement through the flexible compensation plan; student health records maintained by the Student Health and Student Counseling centers; and health forms submitted by student-athletes.

In compliance with the provisions of HIPAA, WPI has developed privacy policies and procedures that assure the confidentiality of any "individually identifiable health information" that it maintains or transmits in any form; that define the circumstances under which the university may use and disclose this information; and that explain how individuals may access their own records. WPI's policies and practices are specific to the types of health records it maintains.

Employee Health Records

WPI's HIPAA Privacy Policy states that the university may use or disclose an employee's health information under limited circumstances (for example, for the purposes of making or obtaining payment for the employee's care or to conduct health care operations), and that disclosures will be limited to the minimum amount of information required. WPI may not disclose an employee's health information for other purposes without that employee's written authorization. Employees have a variety of rights under HIPAA, including the right to restrict certain uses of their health information and certain types of disclosure; the right to inspect and copy their information, and the right to amend their information if it is inaccurate or incomplete.

WPI's HIPAA Privacy Policy:
www.wpi.edu/Admin/HR/BenMan/privacy.html

Student Medical Records

WPI treats all student health information as confidential and will not disclose it to a third party (including parents, spouses, and college officials) without the student's written consent. There are limited exceptions to this policy: WPI may disclose information in situations where there is a threat of imminent harm to self or others. In addition, WPI may be obligated to report to public health officials information about students who have contracted certain communicable diseases.

WPI's Student Health Center Confidentiality Policy:
www.wpi.edu/Admin/Health/Eligibility

Massachusetts law requires all full-time and qualifying part-time students to have primary insurance coverage for sickness and accident claims. Therefore, WPI requires students to either provide proof of coverage meeting Massachusetts' qualifying student health insurance program (QSHIP) requirements, or to purchase coverage under the Student Health Insurance Plan for WPI, currently administered by Student Resources Insurance. Student Resources Insurance handles all records related to student health insurance claims.

Student Resources' Privacy Policy:
www.studentinsurance.net/public/Privacy.asp

Financial Records

Gramm-Leach-Bliley Act (GLBA)

The GLBA requires financial institutions to safeguard and protect the privacy of customers' personal financial information, whether that data exists on paper or in electronic form. Since WPI administers student loans and handles financial information provided by students and their families, the university is covered by the provisions of this act and takes seriously its obligation to protect the financial data it maintains.

As required by GLBA, WPI has identified and addressed security risks associated with its storing, handling, and disposing of financial data, designed and implemented safeguards to control those risks, trained employees who handle financial data to maintain the security of that information, and required third-party service providers that handle the personal financial information of students, parents, employees, and other parties connected to WPI to comply with the provisions of GLBA.