University System of New Hampshire

USNH CYBERSECURITY POLICY OVERVIEW AND MAPPING

KSC - IT SECURITY: FEDERAL, STATE OR LOCAL LAWS MAPPING

Current Policy: https://www.keene.edu/administration/policy/detail/it-security-federal-state-or-local-laws/

The IT Group will cooperate fully, upon the advice of the College legal counsel, with any local, state or federal officials investigating an alleged crime committed by an individual using Keene State College information technology resources.

- **NP** = 5.3.7, 5.9.1, primarily covered in the new USNH Acceptable Use Policy
- **ST** = Access to Password Protected Information Standard

All existing federal, state, or local laws apply to Keene State College computer and network use. Laws relating to privacy and information technology have become complex. There is no single, comprehensive set of computer use and/or network use laws but there are a few laws specifically applicable to college or university computer use. The Educause Computer and Network Security Task Force published IT Security for Higher Education: A Legal Perspective (The excerpts below were extracted directly from the EDUCAUSE/Internet2 Computer and Network Security Task Force web site) and identified the following laws specifically pertinent to colleges and universities:

- **NP** = 5.9

Family Education Rights and Privacy Act (FERPA)

FERPA is the keystone federal privacy law for educational institutions. FERPA generally imposes a cloak of confidentiality around student educational records, prohibiting institutions from disclosing "personally identifiable education information," such as grades or financial aid information, without the student's written permission. FERPA also grants to students the right to request and review their educational records and to make corrections to those records. The law applies with equal force to electronic records as it does to those stored in file drawers. While violations of FERPA do not give rise to private rights of action, the U.S. Secretary of Education has established the Family Policy Compliance Office which has the power to investigate and adjudicate FERPA violations and to terminate federal funding to any school that fails to substantially comply with the law.

To learn more about FERPA, go directly to the U.S. Department of Education FERPA Web pages.

- **NP** = 5.9
- **ST** = Protected Information Handling Standard

Electronic Communications Privacy Act (ECPA)

The ECPA broadly prohibits the unauthorized use or interception by any person of the contents of any wire, oral or electronic communication. Protection of the "contents" of such communications, however, extends only to information concerning the "substance, purport, or meaning" of the communications. In other words, the ECPA likely would not protect from disclosure to third parties information such as the existence of the communication itself or the identity of the parties involved. As a result, the monitoring by institutions of students' network use or of network usage patterns, generally, would not be prohibited by the ECPA.

- *The intent of this provision is covered in the USNH Acceptable Use Policy, this type of information isn't appropriate for a Policy/Standard as it is informational not prescriptive*

Computer Fraud and Abuse Act (CFAA)

The CFAA criminalizes unauthorized access to a "protected computer" with the intent to obtain information, defraud, obtain anything of value or cause damage to the computer. A "protected computer" is defined as a computer that is used in interstate or foreign commerce or communication or by or for a financial institution or the government of the United States. In light of the "interstate or foreign commerce" criterion, the act of "hacking" into a secure web site from an out-of-state computer, which may have occurred when the Princeton admissions officer accessed Yale's "secure" web site, could be considered a CFAA violation (although both schools took pains to say that they were not seeking any civil or criminal prosecutions). The fact that both ECPA and CFAA are criminal statutes considerably raises the ante.

- *The intent of this provision is covered in the USNH Acceptable Use Policy, this type of information isn't appropriate for a Policy/Standard as it is informational not prescriptive*

USA Patriot Act

The USA PATRIOT Act, passed six weeks after September 11, 2001, grants law enforcement increased access to electronic communications and, among other things, amends FERPA, ECPA and the Foreign Intelligence Surveillance Act of 1978 (FISA), in each case making it easier for law enforcement personnel to gain access to otherwise confidential information. Perhaps most significant in the context of higher education is an amendment that potentially prohibits institutions from revealing the very existence of law enforcement investigations. Under Section 215 of the USA PATRIOT Act, which amends Sections 501 through 503 of FISA, the FBI can seize with a court order certain business records pursuant to an investigation of "international terrorism or other clandestine intelligence activities," and record-keepers are prohibited from disclosing the FBI's action to anyone "other than those persons necessary to produce the tangible [records] … ." The same goes for investigations into data banks storing information, such as information about who may have accessed certain library resources - thus, librarians may not even reveal that an inquiry has been made.

The Educause Web pages have several USA Patriot Act documents in their resource library.

- *Removed, this type of information isn't appropriate for a Policy/Standard as it is informational not prescriptive*

TEACH Act

The TEACH Act, signed into law on November 2, 2002, relaxes certain copyright restrictions to make it easier for accredited nonprofit colleges and universities to use materials in technology-mediated educational settings. But the new law carries with it obligations that have privacy and security implications: institutions that want to take advantage of the relaxed copyright restrictions must limit "to the extent technologically feasible" the transmission of such content to students who actually are enrolled in a particular course, and they must use appropriate technological means to prohibit the unauthorized retransmission of such information. In other words, the TEACH Act may require institutions to implement technical copy protection measures and to authenticate the identity of users of electronic course content.

- Removed, this type of information isn't appropriate for a Policy/Standard as it is informational not prescriptive

Digital Millennium Copyright Act (DMCA)

The 1998 enactment of the Digital Millennium Copyright Act (DMCA) represents the most comprehensive reform of United States copyright law in a generation. The DMCA seeks to update U.S. copyright law for the digital age for ratification of the World Intellectual Property Organization (WIPO) treaties. Key among the topics included in the DMCA are provisions concerning the circumvention of copyright protection systems, fair use in a digital environment, and online service provider (OSP) liability (including details on safe harbors, damages, and "notice and takedown" practices).

Read and learn more about the DMCA.

- **NP** = 5.9
- **ST** =
    - DMCA Compliance Standard (future)

About this Policy
IT Security: Federal, State or Local Laws
Ownership: Information Technology
Last Modified: Jul 25, 2019