

# Appendix 13

## US Patriot Act Information Request

### Introduction

The U.S.A. PATRIOT Act was enacted on October 26, 2001, in response to the terrorist attacks of September 11, 2001. The Patriot Act is designed to broaden the surveillance capabilities of law enforcement agencies in an effort to achieve early detection of potential terrorist plots. Pursuant to the provisions of The Patriot Act and acting under the authority of a valid court order, law enforcement agencies may request various forms of information, records, documents or data from institutions of higher education. Such data includes, but is limited to, records of borrowed print materials, records of internet access, email communication records and telephone usage records. The Patriot Act authorizes law enforcement agencies to install devices to monitor computer access and telephone usage, at the enforcement agency's expense, in libraries and/or information systems departments if necessary to implement the purposes of the Act.

The provisions of The Patriot Act supersede Tennessee law regarding the confidentiality of library records. Under Tennessee law, a public patron's library records are not public records. Such records are classified as confidential, and library personnel may only disclose the content of those records in certain circumstances permitted by law. Tennessee law permits disclosure of a public patron's library records if: (1) the patron consents; (2) the library must disclose the information to obtain reimbursement for the return of lost or stolen materials; and/or (3) the records requested are pursuant to a court order. In addition to the aforementioned circumstances delineated by state law, The Patriot Act specifies that confidential library records of a patron must be disclosed if a legitimate request for such records from a law enforcement agency is provided as required by the Act.

### Institutional Policy

#### A. Record Maintenance and Retention

Records of personal computer identification accounts that require individuals to log onto the campus system may be subject to review by a law enforcement agency under The Patriot Act. NSCC will maintain accurate computer usage logs, and retain the records in accordance with state mandated record retention guidelines for the college. Records shall not be destroyed prior to the date authorized by the retention guidelines, or as a method to avoid compliance with an official request for records.

NSCC issues each student and employee an individual computer identification account (log in name and password) for access to the institution's computer network. The maintenance of accurate computer usage logs occurs electronically through the individual user's log in/log out process. In the event that law enforcement officials request information regarding general computer access or a specific individual, NSCC shall comply with the request by searching its electronic database of authorized users' log in access to the network.

NSCC informs network users, in its computer use policy, of their responsibility to consistently utilize the log in/log out procedures when accessing the institution's computer network. Users are also informed that they are responsible for any computer files, databases, and/or internet sites that are accessed through their computer identification account, notwithstanding their failure to adhere to the log in/log out process, or their voluntary publication of their account information to others.

### **B. Voluntary Reporting of Suspicious Activity**

The Patriot Act authorizes voluntary disclosure of the contents of electronic communication to law enforcement officials if the provider reasonably and objectively believes that the institution's computer system has been compromised such that an emergency involving immediate danger of death or serious physical injury may occur without disclosure to a law enforcement agency. Personnel suspecting a breach of the institution's computer network should discuss the concern with the department's director/dean, providing appropriate documentation or evidence if available. The director/dean shall investigate the situation. The director/dean shall then consult with the appropriate vice president prior to disclosure to law enforcement.

### **C. Users Notice**

NSCC will post notices to users in its computer laboratories informing them that The Patriot Act authorizes law enforcement agencies, acting pursuant to a valid court order, to compel personnel to disclose confidential information about their electronic communication via email; their computer access of the internet and other network databases; and/or records of their telephone usage.

### **D. Employee Training**

Training of all staff (including student employees and volunteers) is necessary for the implementation of this policy. Departments shall provide all employees a written copy of the policy and adequate training regarding the policy to understand their roles in its implementation.

## **Response to Requests from Law Enforcement**

In any situation in which a law enforcement agency requests previously documented information pursuant to a court order, search warrant, or subpoena; and/or any type of assistance in monitoring information in the future, administrators should contact the Vice

President of Academic Affairs. Upon his/her arrival at the institution, the law enforcement officer shall be directed to the Vice President of Academic Affairs who is responsible for directly communicating with officials. In the absence of the Vice President of Academic Affairs, the Vice President of Community/Economic Development shall be responsible for acting on her behalf.

If a law enforcement officer presents a court order (i.e., warrant or subpoena), the Vice President of Academic Affairs shall do the following: (1) cooperate with the officer (after verifying that he/she is properly affiliated with a legitimate law enforcement agency and requesting the information for action within the scope of his/her employment with that agency); (2) implement the appropriate steps of the institution's policy.

The Vice President of Academic Affairs will maintain accurate, comprehensive, and confidential written documentation of each request for information from law enforcement personnel.

## **FERPA**

The Patriot Act amended certain provisions of the Family Educational Rights and Privacy Act (FERPA). Specifically, the amendments grant educational institutions the authority to disclose, without consent or knowledge of the student or parent, personally identifiable information from the student's education records to the Attorney General of the United States or his designee in response to a court order (ex parte order from the Attorney General, grand jury subpoena, or law enforcement subpoena) in connection with the investigation or prosecution of terrorism crimes. Under The Patriot Act, an institution of higher education will not be held liable to any person for the production of educational records to law enforcement personnel in accordance with an order issued under The Patriot Act if the institution acts in good faith. Moreover, the amendment to FERPA does not require the institution to record the disclosure of information from a student's education record when making a disclosure to a law enforcement agency under The Patriot Act.