1975 Inter-Action 2005

SPECIAL EDITION: Privacy Issues

A Publication of AAUP-KSU **July 2005**

The Stolen Laptop: What is Being Done?

In June, a laptop computer containing sensitive data was stolen from the car of Alvin Evans, Associate Vice President for Human Resources, outside of a Walmart store. The laptop contained names, Social Security numbers (SSNs), birth dates, titles, and disciplinary affiliations for some 820 tenure-track and other faculty. The data did not include a field indicating AAUP-KSU membership status, and the group as a whole included members and non-members. The file was prepared in order to compare data about KSU faculty disciplines with information provided by the National Association of State Universities and Land Grant Colleges (NASULGC). It had no special application to bargaining or relations with the unions on campus. A separate file included payroll information pertaining to members of the AFSCME bargaining unit. Both files dated to 2001. Both were located in the "trash" of the operating system and apparently had not been properly deleted. AAUP-KSU Grievance Chair Jennifer Larson contacted Greg Seibert, the University's Director of Security and Compliance, to ask what is being done to safeguard KSU employees' information.

Short term	***Long term***
Affected employees received a letter notifying them of the problem and advising them to have an initial fraud alert placed on their SSNs. This means that a statement is added to one's credit report warning future creditors to verify identification before opening new accounts. Typically, an initial fraud alert stays in place for 90 days and is renewable and free.	The University will switch as soon as possible to a new information system that does not use SSNs as identifiers for employees. Currently, there is an effort underway to identify the best option for making such a switch. A completely new system has an estimated price tag of $20 million, while it would cost considerably less to adapt the current system. The change is expected to take place in 1-5 years.
The University has negotiated further protection with Equifax on behalf of affected employees, who will be able to sign up for an additional year of "Credit Watch" protection at the University's expense. Mr. Seibert counseled against purchasing other extra fraud protection services offered by the credit agencies. To our knowledge, nobody has yet made use of any of the lost information to commit fraud.	New policies and guidelines are being formulated to address the proper handling of sensitive information, and the laptop incident will be taken into account. Specifically, there is a plan to register and track all portable devices on which sensitive data is stored (not just laptops but PDAs and memory devices). Mr. Seibert is also working to make file encryption standard for sensitive data.

Resources on identity theft

For a free DVD from the US Postal Service on Identity Theft and Fraud, visit http://shop.usps.com/cgi-bin/vsbv/postal_store_non_ssl/home.jsp and use the search term "identity crisis."

Check out KSU Security Director Greg Seibert's website for policies, security updates and notices of upcoming workshops: http://www.kent.edu/administration/is/security/

How to protect your students

The privacy of student educational records is regulated by FERPA, the Family Educational Rights and Privacy Act (1974). Here's how you can stay in compliance with FERPA and help ensure that student information remains private.

DO:

- Exercise special care when transporting laptops or other portable devices with files that include student grades (this will become more important as the University makes laptops the standard for the computer refresh program).
- Where possible, use a system for identifying students that does not involve SSNs.
- Insist on written permission from the student before releasing information about grades or student progress to any person outside the University, including parents.
- Respect the privacy of students with health problems by keeping these confidential.

DON'T:

- Ask students to write their SSNs on exam papers or otherwise reveal their SSNs.
- Post grades publicly so that students know each other's grades, or post rosters that include SSNs.
- Allow students to pick up graded papers for their friends.
- Provide anyone with information about a student's schedule or assist anyone other than a University employee with finding a student on campus.
- Share educational information about individual students with other faculty or staff unless they have a need to know in the course of their duties.

AAUP-KSU
1100 E. Summit St.
Kent, OH 44240
330-673-9118; 330-673-2142 (fax)
aaupksu@kent.edu

Not as private as you think: some answers to faculty questions about privacy on the job

Is my email private?
Not really. The University recognizes the private nature of email in principle, and University Policy says that the privacy of employees' email should be respected. However, the University may access email files in the normal course of maintaining the network, or if it has reason to suspect violations of policies or laws. Also, email sent on the KSU servers falls under the definition of public records. Anyone may make a request for information under the Ohio Public Records Act. If someone makes a specific request involving your email, the University must comply, though it is expected to make a good-faith effort to notify the affected user. Therefore, the best way to protect yourself is to avoid sending email of a personal nature through the KSU servers. Obtain an account from an independent service such as Yahoo or Hotmail. If you are writing something that you would feel uncomfortable having others read, don't send to or from a kent.edu account.

How private is my office?
According to policy 3342-5-303, offices assigned to individual employees may be entered (1) with proper authorization from the occupant; (2) if another employee needs to enter the office in the performance of his or her normal duties (custodial or maintenance worker, police officer, etc.) or (3) with written permission of the appropriate Vice President. Because this type of entry into a Faculty member's office is rare, many Faculty may not be aware that their offices can be entered without notice.

What about my computer files?
In general, files stored offline on computers owned by the University have a higher degree of protection than email, as they are not considered public records. However, computers are analogous to employee offices. Under certain rare circumstances, the University may find it necessary to access your computer files and it has the legal right to do so. University employees who maintain the computers may also view files in the course of their work; they are expected to maintain the confidentiality and privacy of any files they see unless otherwise required by policy or law.

In the case of files that are posted on the Web or transmitted via networks, the stated policy (3342-5-41) is that the University generally shall not monitor or restrict their content. However, the University reserves the right to remove or limit access to websites when there is evidence that they violate existing policies, laws, or contracts. There is a special prohibition on using University-owned computers or networks to harass or defame another person.

The best way to protect your files is to periodically back them up onto a device that you own. Do not store files of a personal nature on your University-owned computer. Also, keep in mind that from time to time people may enter your office in the course of their duties. To protect against unauthorized access to your files, keep them password protected, avoid posting the password on or near the computer, and change the password regularly.