Computer User Caveats

Most would find it difficult to imagine doing their jobs without computers. The hobbies and pastimes of many center around computers. As valuable and essential as computers are, their use carries with it some risks. A number of the more commonly encountered risks are discussed below.

1. Use of E-Mail in Discussions of Personnel Matters

In only a few minutes, an e-mail message can be sent at virtually any time of the day or night, from almost anywhere, without regard to whether the recipient is in his/her office, or even in the country. This allows a message to be sent at the convenience of the sender and read at the convenience of the recipient. This functionality effectively puts an end to "telephone tag" and to the need to take notes during or prepare a memorandum following a telephone conversation. Such convenience has helped e-mail become a common tool for communication on the University's campus, as elsewhere.

Increasingly, e-mail is becoming a major focal point for plaintiffs during the discovery phase of a lawsuit. It is not uncommon for an e-mail message to provide the "smoking gun" in suits alleging employment discrimination, defamation, invasion of privacy, etc. As a result, anyone considering using e-mail to communicate information or opinions regarding any personnel matter should consider carefully whether use of e-mail is appropriate. In making that assessment, it is wise to assume that everything contained in that message will become known to all of those individuals directly or indirectly affected by the decision made in that personnel matter.

E-mail may still be used to provide information to the Office of Counsel for the purpose of obtaining advice, so long as copies of that e-mail are not sent to others who are not providing legal advice regarding the matter dealt with by the message. Such e-mail will be protected by the attorney-client privilege. However, even such a practice is not without hazard since mis-typing an e-mail address by a single character can result in the wrong person receiving the message.

2. Use of Social Media Sites

Sites such as Facebook have hundreds of millions of users. Those users are commonly intertwined through "friending" connections, so that a Facebook posting is typically made known instantly to the public at large or, at the least, to a group of individuals.

Increasingly, employers are implementing social media policies which provide restrictions on what employees may post on their personal accounts regarding their employer and work activities. Violations of those restrictions may result in disciplinary action. Even in the absence of a social media policy, an employee who is "at-will" may be fired as a result of social media postings that portray the employer unfavorably. Employees who post public criticisms of

their supervisors may also find themselves sued by the supervisor for defamation of character.

Many employers are also reviewing Facebook postings as part of their pre-employment screening of job applicants. In come cases, employers require the applicant to provide username and password information to permit the employer access to accounts that are not viewable by the public.

3. Use of Laptop Computers

Laptop computers make it possible to carry vast amounts of information easily from place to place. These computers are frequently used to carry information between work and home and while on trips, both within and outside the U.S. Unfortunately, laptop computers are frequently lost or stolen, particularly in airports. If this does occur, the adverse impact can be mitigated, sometimes eliminated, if the information has been appropriately encrypted.

The Family Educational Rights and Privacy Act (FERPA) imposes special obligations on the University to maintain the confidentiality of personally identifiable information regarding students, while the Health Insurance Portability and Accountability Act (HIPAA) imposes similar obligations to maintain confidentiality of personal health information. Storage or transportation of information protected by FERPA or HIPAA on laptop computers should not take place unless the information is encrypted.

Some information contained on laptop computers may be subject to the restrictions of the Export Control Act requiring a license prior to taking that information outside the country. Other information may be subject to non-disclosure agreements that would be violated if the laptop computer is lost and the non-discloseable information is not encrypted.

4. Use of University Computers for Personal Purposes

De minimis use of University computers for personal purposes is unlikely to result in adverse action so long as the use is legal, does not interfere with performance of work duties, and takes place outside of work hours. However, using a University computer to conduct unauthorized commercial activities, such as the operation of a private business, would violate the University's General Computer Use Policy. Use of a University computer to view obscene materials at any time would also violate that Policy.

5. Use of University Computers in Violation of Copyright Laws

The University requires compliance with copyright laws. Failure to comply subjects a University employee or student to disciplinary action. Additionally, there are both civil and criminal penalties for copyright violations. In the case of a willful violation of the copyright law, a court may award damages of up to $150,000.00 per copyright infringement. Willful violations may also be pursued as a criminal matter that can, in a worst case, result in imprisonment for as long as ten years and a $250,000.00 fine.

6. Use of Computers in Violation of Obligations to Preserve Evidence/Public Records

When a civil lawsuit has been filed against the University or when it can be reasonably anticipated that one will be filed, the University is required to take steps to identify, locate, and preserve documents (both in paper and electronic formats) that are themselves relevant to the actual or anticipated lawsuit or that may reasonably lead to the discovery of admissible evidence. Lawyers from the Office of Counsel (and outside legal counsel in some cases) will meet with those employees who are determined to have evidence that must be preserved and provide guidance regarding what must be done and what cannot not be done in order to meet the University's obligation to preserve evidence. Following this meeting, written instructions (frequently referred to as a "litigation hold") will be provided. It is essential that the requirements of the litigation hold be met. A failure to do so would subject the University employee to disciplinary action and could result in judicial sanctions against both the University and the employee. Sanctions against the University include payment of plaintiff's costs in responding to the failure to preserve information, denying the University the right to call a witness, or even a directed verdict in favor of the plaintiff.

Independent of the duty to preserve evidence pertaining to on-going or reasonably anticipated litigation, offices and officials of the University have an obligation to record and maintain records of their official acts. While not bound to do so, the University voluntarily follows the Functional Analysis and Records Disposition Authority guidance issued by the Alabama Department of Archives and History. That guidance should be followed in the management/retention of electronic records as well as paper documents.

All of the risks discussed above are readily manageable. They are simply the cost of doing business in the Digital Age.