0041-A

ANTIOCH UNIVERSITY

E-MAIL POLICY FOR TRUSTEES AND OFFICERS

This e-mail policy has been adopted to protect the University's interest when Trustees and Officers communicate using e-mail and internet access to conduct Antioch University business.

This policy applies to each member of the Board of Trustees, Members of the ULC and to all officers of the University. It is intended to serve as guidance for the Board of Trustees, Members of the ULC and to all officers of the University.

Members of the Board, ULC and all officers of the University conduct Board business utilizing the internet-based electronic mail (e-mail). The legal risks require us to exercise special caution when communicating by e-mail. Please exercise proper judgment in the use of Antioch University Board business e-mail.

This policy reminds us that the use of e-mail should be restricted to those with a need to know. E-mail communication has a shelf life far beyond that of paper communication and should be considered confidential and discoverable in the event of litigation or a government investigation. Therefore, all e-mail should be written so that a reasonable person would not find it to be defamatory, offensive, harassing, or derogatory.

This policy expressly prohibits sending to, forwarding or copying Antioch University Board business e-mail communication to persons without a need to know and/or without the consent of the sender.

This policy further suggests that Antioch University Board business e-mail be erased from your computers at least every thirty (30) days.

MEMORANDUM

TO: David A. Weaver

FROM: Regina Watson

DATE: July 26, 2002

RE: Antioch University: Unregulated Use of E-Mail for Board of Trustees Business

---

Three may keep a secret, if two of them are dead.
- Benjamin Franklin

We have been asked to address legal considerations pertaining to the unrestricted and increasing use of Internet-based electronic mail ("e-mail") by University Board of Trustees members in conducting Board business. We conclude that legal risks grow exponentially with the proliferation and unreflective use of e-mail in such a context.

E-Mail's Special Characteristics

E-mail interaction offers special characteristics which make it a peculiarly risky mode of business communication from a legal standpoint. Here we review some of the characteristics which require us to exercise special caution when communicating by e-mail.

First, virtually any e-mail can be sent, re-sent, and forwarded to a large number of recipients easily and instantaneously, on a global scale, at practically no additional financial cost to the sender. The point-and-click simplicity of dispatching e-mail messages greatly increases the likelihood that a message mistakenly will be sent to an unintended recipient, or hundreds of unintended recipients, without the sender's immediate knowledge.

Second, the shelf life of e-mail messages, in contrast to postal correspondence, often is unknown and virtually unknowable to both the sender and the recipient. On the one hand, e-mail messages can be extremely fragile and ephemeral. Retention and destruction of e-mail messages often occurs without the volition, or even the knowledge, of the corresponding parties. An e-mail message containing significant, sensitive information accidentally may be deleted as junk mail by the recipient with no option to recover a copy if the need arises some weeks later. Some computer systems automatically delete aging e-mail messages unless the user takes affirmative action to prevent the deletion. Computer and server "crashes" also may destroy significant

numbers of e-mail messages, with recovery capabilities dependent upon the types of back-up systems, if any, previously deployed by the users.

On the other hand, e-mail messages can last almost forever, even without heroic efforts to preserve them. A user may have difficulty in tracing and destroying all copies of an e-mail message even when the user is intent on such destruction. Supposedly "deleted" e-mail messages and attachments may survive on computer hard drives until overwritten by the storage of new information. Such "deleted" but not overwritten messages may be recovered using special software programs. Additionally, extra copies of "deleted" e-mail messages may reside for months or years on the sender's, the recipient's, or a third-party's computer server. Likewise, an e-mail message may be stored on backup tapes or otherwise archived for years, decades, or even longer by any party sending, receiving, or transmitting a copy of the message. Where a third-party service has backed up the data, the users lose control over their retention of the content. The third party service may retain backups for a short period, such as 30 days, or for several years for recovery in case of catastrophic damage to the computer system. Alternatively, the third party may keep the full backup only until the next business day (when the next full backup is completed). With the click of a mouse, any user can print a large number of "hard copies" of e-mail messages and their attachments. These hard copies end up tucked away in a variety of formal and informal paper filing systems maintained by various individuals and/or their institutions and may be scanned back into electronic form at a later time.

Third, e-mail records are exponentially more portable and more accessible than paper records. For instance, e-mail records can reside on a laptop or on a network system linking multiple personal computers, may be copied multiple times on diskettes , or retrieved via the Internet.

Fourth, it is far more convenient to store a vast amount of information in electronic form such as e-mail messages than in traditional paper records. The volume of information on a few CD-ROMS, for example, could amount to a warehouse full of boxes if the information were stored in paper form. With the right search tools, of course, it also is far easier to review and retrieve documents from electronic media than to wade through a warehouse full of boxes of paper files. Many organizations discover that electronic records are being retained far longer than needed or desired partly because records stored in electronic require much less physical space than records stored as paper.

Fifth, e-mail messages are more susceptible to data corruption, subtle tampering, manipulation of date and time stamps, unauthorized disclosure, and interception than are some traditional means of business communication. In particular, e-mail communications are peculiarly prone to eavesdropping and surveillance. While no communications method in common use is completely risk free, e-mail in some ways is riskier than phone calls, postal mail, faxes or couriers. The low risk that an eavesdropper will be detected, let alone caught, let alone prosecuted and punished, makes e-mail surveillance much more attractive to sophisticated spies than are

alternative methods such as wire-tapping an organization's telephones. Furthermore, e-mail surveillance can be significantly less expensive than other methods of eavesdropping. The analysis of large amounts of recovered information can be automated through the use of any number of computer programs designed for that purpose.

Last but not least, many e-mail users erroneously believe that e-mail is as private as face-to-face conversation and that they accordingly are justified in communicating anything they may please in any manner they may please. Individuals communicating by e-mail often use language and make compromising statements which might be appropriate for private internal conversations but which are totally inappropriate for formal written documents which may be scrutinized by outside parties. The informal nature of e-mail communication means that e-mail messages typically are poorly proofread for spelling, grammar, and even substantive content. Indeed, the ability to compose and send e-mail in a matter of seconds without secretarial assistance enables users to engage in reckless exchanges due to anger or other spur-of-the-moment emotional impulses. The freer and sometimes promiscuous distribution of institutional information promoted by e-mail's ease of use invites comments and editorials by a host of individuals who may act beyond the bounds of their institutional role or personal qualifications. An article by attorney Gilbert Keteltas, aptly describing the pitfalls of this approach, is attached to this memorandum.

Several highly publicized horror stories have illustrated the risks of e-mail communication. A recent investigation into Wall Street's business practices revealed what one Merrill Lynch financial analyst apparently thought about impartiality. "The whole idea that we are independent from banking is a big lie," he stated. A probe by New York's Attorney General, Elliot Spitzer, allegedly captured such analyst privately admitting that he and his colleagues sometimes were more interested in attracting banking fees than objectively analyzing the value of businesses. Another analyst reportedly stated that a company being advertised to the public as an investment vehicle actually was "a piece of junk." These apparently damaging statements were discovered in e-mail messages previously sent by the financial analysts and still recoverable at the time of the Attorney General's investigation. In another well-known example, e-mail messages revealed Microsoft Chairman Bill Gates' candid opinion regarding Netscape. In a third high-profile illustration, Special Prosecutor Kenneth Starr recovered personal e-mails which Monica Lewinsky attempted to delete from her computer hard drive, and this information made it way into Starr's impeachment report.

In short, various aspects and peculiarities of e-mail tend to magnify the legal risks of business communication. Large numbers of hasty, ill-informed, or simply imprudent messages, attachments, and commentary, existing only momentarily or persisting indefinitely in likely and unlikely locations, will increase dramatically the probability that damaging evidence will be created and later exploited to harm an institution in a legal inquiry or proceeding. This situation also increases the probability that the institution will fail to marshal the e-mail material which, at least in theory, is

under the institution's control, when the institution needs to do so in the course of a legal inquiry or proceeding.

Legally Compelled Disclosure

As part of the litigation process, public and private litigants are entitled to obtain information from both parties and non-parties to the litigation through a process known as "discovery." Unless a special exception applies, information generally is subject to compelled disclosure through discovery if the information is reasonably calculated to lead to evidence relevant to the litigation. Courts have been ordering the preservation, discovery and admission of electronic evidence since at least the mid-1970's. For the most part, the discovery principles applicable to paper-based records also are applicable to electronic-based records such as e-mail messages. As with traditional paper discovery, the courts appear to be very generous in permitting broad discovery of electronic data.
Courts often order the production of computerized records in a usable electronic format, and inaccessibility does not relieve an institution from its responsibility to make information available.

A discovering party generally may physically inspect and check the original electronic sources of information available in other formats. The party often is entitled to an on-site inspection at the institution's place of business. The more extensive and the more poorly organized an institution's electronic records, the more time-consuming and invasive such an inspection will be for that institution.

Under the doctrine of spoliation, when litigation is imminent or when a party has reason to believe that litigation is likely, the party has a duty to preserve evidence pertaining to the dispute. This duty arises even before the other party has requested access to the evidence. Thus an institution must anticipate having to locate and preserve relevant documents very early in a known dispute likely to lead to litigation.

Penalties for unjustifiable destruction or "spoliation" of evidence include adverse inferences or presumptions, preclusion of evidence which otherwise would be admissible, monetary sanctions, and dismissal or default. Judges and juries hearing a case are permitted to infer that a party who destroyed potentially relevant evidence did so out of a realization that the evidence was unfavorable to that party. In several jurisdictions, spoliation also gives rise to a separate cause of action in tort. Ohio is one of only a few states which recognize the tort for negligent destruction as well as intentional destruction. At the federal level, criminal penalties apply to obstruction of justice through destruction of evidence. Thus an institution on notice of potential litigation can expose itself to the risk of costly and damaging sanctions if it fails to preserve pertinent electronic information stored under the institution's control.

Sanctions are available even where the destruction is unintentional. Thus, for example, if a university fails to halt routine destruction of aging e-mail messages when

the university knows or should know that these records may have evidentiary value for impending litigation, the university is subject to sanctions despite the lack of bad intent.

Clearly, when litigation may be imminent, the destruction of any potentially relevant electronic files should be halted immediately. As noted, once notice has been received, the duty to preserve evidence applies not only to what may have been requested up to that point but also to 1) what one knows or reasonably should know is relevant or reasonably calculated to lead to the discovery of admissible evidence, and 2) what is reasonably likely to be requested. If all pertinent electronic information is not identified early in the litigation, such evidence may be overwritten or erased during the normal operation of the computer system or the rotation of backup tapes. Liability for spoliation can be avoided if materials destroyed prior to notice are destroyed only in accordance with a neutrally applied records retention policy and if the institution follows a policy containing proper procedures to follow after notice of a claim has been received.

Apart from spoliation sanctions, there can be other costs for poor management of electronic information which turns out to be potentially relevant in subsequent litigation. If evidence harmful to the institution initially cannot be located but is divulged later in the litigation, the situation exposes the institution to charges of orchestrating a deliberate coverup. However unfair these charges may be in reality, they can play a decisive role in jurors' minds.

The same considerations apply in relation to a government agency's subpoena powers. The institution's computer files may be mined for communications which the institution, in retrospect, wishes had never seen the light of day. Conversely, the institution may not be able to shift through and marshal its virtual mountains of electronic information so as to produce a legally adequate and strategically optimal response in the time available.

Moreover, it is not only the institution's own electronic records which are subject to discovery and search by public and private entities. Electronic records on employees', trustees', and other individuals' private computers also are vulnerable to being subpoenaed if potentially relevant to litigation or a government investigation. Needless to say, in all these situations, the institution's defensive and offensive tactics can be greatly complicated, or rendered completely unmanageable, by a history of indiscriminate e-mail communication.

Records Creation and Retention: Policies and Procedures

Many electronic data problems, such as exposure to discovery sanctions, tort claims and other liabilities for spoliation are diminished if records are maintained and disposed of in conformity with a formal records retention policy. Plainly a document retention policy should not be burdensome to daily efficiency but should offer easy-to-follow guidelines. An effective policy is designed to identify and preserve necessary business documents and to retrieve electronic records for litigation, while keeping the

total volume of records in storage to a minimum. Such a policy should be tailored to achieve the institution's legitimate corporate objectives. In addition to reflecting legal and regulatory requirements, the institution's record retention policy should reflect the following goals: cost-effective management to support ongoing organizational activity; protection of vital electronic records needed in case of disaster; security of private, confidential and proprietary information; preservation of records having long-term and historical value; accessibility of records relevant in foreseeable, judicial, regulatory, congressional and other legal proceedings; and procedures for proper disposition of "non-records" and records beyond their retention periods.

Records destruction should be performed on schedule and documented using a form developed for that purpose. Thereafter, if questions arise concerning the circumstances under which the destruction took place, the disposition form will reveal that it took place in compliance with the neutrally administered retention policy.

A good records retention policy prevents obsolete, unnecessary, or potentially harmful documents from lingering just long enough to be subject to discovery requests. The policy also provides a defense if allegations of spoliation arise. If a document destruction issue arises, the institution can assert that the document was destroyed in good faith in accordance with the neutral records retention policy.

Such a policy is especially important for e-mail messages, because it can be costly for an organization to produce the huge volume of e-mail messages which typically are generated. Beyond keeping detailed records of document retention and destruction, institutions need a plan in place for the retrieval and preservation of electronic documents when it becomes apparent such documents may be needed as a result of litigation. Institutions often find it difficult to cope with discover requests requiring searches of vast amounts of e-mail. Regrettably, organizations often fail to consider and determine an appropriate records retention period for e-mail communications prior to such a crisis. Some computer system operators believe that backup information should be retained for long periods. There may be, for example, no established procedures to delete e-mail from backup tapes. In that situation, if a discovery request requires production of all communications between specified individuals or relating to specified topics, a collection of backup tapes of e-mail records accumulated over a number of years creates a significant burden and possibly poses significant legal hazards. As noted above, documents which never were "saved" or which were "deleted" still may be retrievable, and therefore discoverable, even though the user is not aware of their existence. "Backups" continue to reside on a user's hard drive and possibly on network servers and third-party servers in addition to data on backup tapes.

Instituting efficient and effective data-retention policies, and using thoughtful methods for storing and retaining electronic information such as e-mail messages, should not only help an institution avoid sanctions but also help it fulfill its discovery obligations. Given the doctrine of spoliation discussed above, the policy should require that all potentially relevant information be preserved until resolution of any pending or anticipated litigation. An effective data-retention policy also organizes computer data,

categorizes information, and provides for an efficient method of searching volumes of stored information to determine relevance when responding to discovery requests under tight deadlines. The short-term investment to implement efficient method of cataloging and referencing stored data such as e-mail messages makes searching for the proverbial needle in a haystack easier and cheaper in the long run. The policy should promote communication between various institutional participants in charge of recycling information, because the duty to preserve evidence attaches as soon as a party knows that litigation is fairly imminent.

In terms of specific steps to cope with the "virtual landfill" of e-mail messages, risk managers suggest a number of procedures that an organization may implement to control the creation and distribution of e-mail, particularly through the Internet, in order to protect the organization from unexpected or inadvertent consequences in case of litigation. Suggested procedures, not all of which may be new or appropriate to the University environment, include the following:

1 Physically segregate backup copies of the e-mail system from backups of the rest of the computer system.

2. Automatically erase e-mail from the computer system, including the backup system, after a short period of time such as 15 to 30 days. As a result, only the most recent backup copies of the e-mail system will continue in existence. Due to the short-term need for e-mail as a substitute for telephone conversations or face-to-face meetings, destruction of all e-mail messages and their backups in a relatively short period is justifiable. However, provide an option to enable users to preserve electronic messages for a limited but longer period of time where necessary. After that limited period of time, e-mail would have to be "formalized" (as described below), or it would be erased automatically.

3. Provide an option to "formalize" certain e-mail messages so that they can be created as or converted into official organization records. Generally these e-mail messages would represent the organization's official position and would be retained in electronic form as the official record. Such a record would be retained in a separate portion of the computer system for the period indicated by the organization's record retention schedule.

4. Maintain the e-mail on one computer system or network, with access provided to others. This procedure reduces the reproduction of e-mail by other systems and reduces the records retention problems while allowing others to participate in the e-mail system.

5. Establish procedures to control the retention of every e-mail message at its source. Stand-alone microcomputers or laptops could contain an executive program or other software product which would impose records retention disciplines similar to the procedures discussed above for e-mail networks. For example, all implicated computers could be equipped with identical e-mail

software which automatically would erase e-mail messages after the specified period of retention. Even the procedures for formalizing records or converting e-mail records to official company records could be incorporated into desktop and laptop computers.

6. Establish writing standards and other rules to impose more careful review of e-mail sent outside the control of the organization. The organization cannot depend on outside parties to implement appropriate retention practices and ensure the timely destruction of e-mail messages. As noted above, records in the possession of another party are subject to litigation discovery and subpoena. (Some advisors recommended that all messages going outside the organization be treated as if they were official organization records and be required to conform to a specified writing standards addressing content, type of language, use of slang, grammar and spelling requirements, prior review, and so forth.)

7. Possibly restrict or prohibit the communication of privileged or highly confidential information by e-mail over the Internet (at least where encryption is not feasible).

In short, good document retention policies reduce the need for resource-consuming file space where documents may languish undisturbed for years until they are exhumed in response to a litigant's discovery request. An effective document retention policy can prevent a jury from seeing and misconstruing a document which may have been harmless when created but which becomes a smoking gun in the hands of a resourceful trial attorney cross-examining a witness with an unreliable memory. However, even the best document retention policy does not prevent the creation of troublesome documents in the first place. To that end, institutional participants would be well advised to learn the rules of "defensive writing," as set forth in the attached article by attorney Gilbert Keteltas. A sound "document creation policy" is as important as an effective document retention policy.

Attorney-Client Privilege

The choice of e-mail communication can compromise the protection afforded by the attorney-client privilege.

The law of attorney-client privilege varies from state to state. The determination of which state's law applies in a specific situation depends on a number of factors. The law applied to a particular communication between attorney and client may be different from the law of the state in which the communication occurred.

In any case, the attorney-client privilege is based on the need to ensure that an individual may confide freely and completely in his or her attorney so as to be adequately represented. Generally, four elements trigger the protection of the attorney-client privilege: 1) the person to whom the communication is made is an attorney acting as such at the time of the communication, 2) the privilege holder is or seeks to become a

client of the attorney, 3) the communication is made for the purpose of obtaining legal assistance, and 4) the communication is made in confidence (with no strangers present to hear the communication). In determining whether a communication was made "in confidence" the intention of the client is controlling. A communication generally is deemed to be confidential where the client has a "reasonable expectation" of privacy and confidentiality. Subject to extremely limited exceptions, attorneys and clients cannot be compelled by subpoena or otherwise to reveal the substance of communications protected by the attorney-client privilege.

Federal law provides criminal and civil penalties for the unauthorized interception or disclosure of any wire, oral or electronic communication. Federal Wire Tap Statute, 18 U.S.C. §2510 et seq. Thus federal law grants to Internet e-mail and other "electronic communications" the same level of privacy that applies to the postal service, commercial mail services, land line telephone communications, and facsimile transmissions. Additionally, various states' ethic opinions and American Bar Association papers have concluded that e-mail messages, even in unencrypted form, afford a reasonable expectation of privacy from a technological and legal standpoint. The ABA Standing Committee on Ethics and Professional Responsibility concluded that e-mail communication poses "no greater risk of interception or disclosure than other modes of communication commonly relied upon as having a reasonable expectation of privacy." The committee further stated that the danger of unintentional interception is not great enough to make the use of e-mail to transmit client confidences per se unreasonable. In short, e-mail communications generally possess sufficient confidentiality to become subject to the protection of the attorney-client privilege.

However, after the attorney-client privilege has attached to a communication, the privilege can be forfeited by waiver. A waiver may be either intentional or inadvertent. For example, if a client discloses to a stranger the substance of what the client told his or her attorney, such disclosure is a waiver of the privilege. On the other hand, unintended third-party interception of an otherwise privileged communication should not constitute a waiver or disqualifying factor with respect to the privilege.

To date, it is not clearly settled whether an inadvertent disclosure, such as accidently e-mailing an otherwise privileged communication to the wrong party, will constitute a waiver of the attorney-client privilege. Under the "Wigmore rule," involuntary disclosures, such as negligent loss of documents from the attorney's possession, destroy privileged status. The reasoning is that because the law has granted secrecy so far as its own process goes, the client and attorney must take reasonable measures to prevent being overheard by third persons. Thus the client would bear the risk of insufficient precautions. The Wigmore rule applies equally to oral statements, paper documents, and electronic documents. For example, some courts have held that attorney-client privilege is lost if otherwise confidential communications are overheard by an eavesdropper; if communications are forwarded, intentionally or otherwise, to an employee outside a privileged group within the client institution; or if communications between lawyer and client inexplicably appear in the possession of a third party.

Accordingly, the greatest danger to the privileged status of electronic communications between attorney and client is simple negligence of attorney or client in hastily preparing, forwarding or replying to e-mail messages. The privilege might be lost through simple failure to confirm that the e-mail is addressed to only appropriate recipients. Although this type of inadvertent disclosure of attorney-client communications is not unique to e-mail, the ability of e-mail irretrievably to be transported to the wrong person, or thousands of wrong people, with the click of a mouse makes e-mail communication particularly hazardous in this regard.

In brief, e-mail communications between attorney and client should be protected by privilege unless a sender accidentally sends an unencrypted version to an inappropriate third party. Such inadvertent disclosures can be avoided by simply checking the e-mail address to make sure it is correct and that only the intended persons are included on the "send," "copy," or "blind copy" line. Senders should be careful not to reflexively click the "reply" button without carefully checking the names and e-mail addresses of all those who will receive the message. Because failure in this seemingly trivial area may result in loss of the attorney-client privilege, use of encryption between clients and their legal counsel may be warranted to reduce the risk.

Trade Secret Protection

Use of e-mail communication can impact an institution's ability to protect its trade secrets.

Trade secrets are governed by state law. A "trade secret" generally is information 1) which derives independent economic value, actual or potential, from not being generally known to and not being ascertainable by proper means by other persons who can obtain economic value from its disclosure or use, and 2) which is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Courts have set forth the following factors as important elements in determining whether a trade secret exists: 1) the extent to which the information is known outside of the institution; 2) the extent to which the information is known by employees and others involved in the institution; 3) the extent of the measures taken by the institution to guard the secrecy of the information; 4) the value of the information to the business and its competitors; 5) the amount of effort and/or money expended by the institution in developing the information; and 6) the difficulty with which the information could be properly acquired or duplicated by others. In requiring that secrecy precautions be reasonable under the circumstances, the highly fact-specific nature of trade secret law imposes an elastic standard of protective conduct. Appropriate levels of security vary on a case-by-case basis.

The question becomes whether transmitting a trade secret by e-mail is consistent with "reasonable precautions" to guard the secrecy of the information. If not, e-mail transmission of the
information may cause it to lose its protected status as a trade secret.

As previously discussed, e-mail and telephonic communications are governed by the same federal statutory scheme making it a federal crime punishable by fine and imprisonment to 1) intercept any electronic or wire communications, 2) intentionally disclose or use the contents of a wrongfully intercepted communication, or 3) wrongfully obtain access to wire electronic communication. Given that interception of e-mail communications, like interception of telephonic communications, is illegal, and that it might be as technically difficult to intercept an e-mail message as it is to intercept a telephone call, it seems unlikely that merely transmitting an unencrypted e-mail message containing trade secret information would compromise a company's reasonable precautions any more than would a telephone conversation communicating that same information.

Nevertheless, a sensitive trade secret or similar information ordinarily should be communicated in a method designed to ensure that no third party has actual access to the information. While the misdirecting of an e-mail message to an unintended recipient should not cause automatic loss of trade secret protection unless the misdirection leads to general availability of the content of the trade secret, the mere possibility of the irreversible loss of trade secret status through such a mistake counsels in favor of extraordinary precautions for transmission of highly sensitive trade secret material. Encryption is advisable.

Conclusion

Unrestricted and reflexive use of e-mail by policy makers transacting University business tends to compromise the institution's ability to prosecute and defend its legal interests. Fortunately, a number of measures are available to ameliorate the situation.