

Privacy Issues & University Internet Monitoring

SIIA has provided a recommended University Internet Usage Policy (<http://www.sii.net/piracy/pubs/UnivInternetUsagePolicy.pdf>) that addresses some of these concerns. It is intended to serve as both a deterrent against wrongdoing as well as an educational tool detailing what is permissible. The level of privacy users (faculty, students, staff) may expect from their computer usage may be curtailed in an effective policy. Having a clearly designed policy will enable the school to protect against wrongdoing and associated liabilities as well as minimize technological threats to the system. These may include harassing or defaming email messages, pornographic postings, copyright infringement, tampering with confidential files, or sabotaging of the network. However, with an effective policy in place, schools can ensure that users know they are not protected by an electronic veil of privacy and that investigations into wrongdoing to identify and sanction the perpetrator may be quickly concluded.

In many cases the actions or omissions of the school may imply a level of privacy. In such cases, a reasonable expectation of privacy may have been established and the school may be held to that standard. The best way to dispel such an expectation is to precisely define what level of privacy users may have and, conversely, what level of involvement the school may have in communications, web sites, postings and other online activity.

Use of a campus computer system is voluntary and as a result, users may be asked to submit to a school policy that successfully achieves this balance as a condition for use. Those that are unwilling to do so, do not gain access to the system. Those users who sign on will know the school's usage policy beforehand, including the fact that their activity may be monitored and possibly used in an investigation, should suspicion of illegal activity arise. In addition, as a campus network is often used to facilitate wrongdoing, the school itself may be held liable for illegal activity occurring on its system. An effective policy may also serve to mitigate against such liability.

Finally, the Electronic Communications Privacy Act (ECPA) which prohibits anyone, other than the sender and the intended recipient of an electronic message, from intercepting, accessing and disclosing its contents has exceptions which specifically enable such investigations. Users cannot attempt to hide behind the ECPA to justify their misuse. The exceptions include:

- **Intercepting:** Electronic communications without the prior consent of at least ONE party. However, consent may be given when the user signs a policy or an on screen message during use can indicate implied consent.
- **Accessing:** Electronic communications except by the entity providing the electronic communications service (i.e. a campus network) or files stored on computers owned by the school.
- **Disclosing:** The contents of an electronic communication except on a need to know basis and/or to comply with an investigation.

SIIA has provided these resources within its Higher Education Initiative in an effort to promote the use of technology in learning. We are confident that in cooperation with colleges and universities we will be able to ensure that technology is used -- not abused.