**Appropriate Use of Information Technology**

[Library name] is committed to ensuring a working and learning environment in which all persons treat others with humanity and respect. Information technology facilities include computing devices and associated peripherals, communications infrastructure and related equipment, FAX machines, scanners, copiers, telephones, video and other multimedia devices and all forms of software.

Such resources and tools are made available to employees in support of their employment and administrative activities and to customers in support of their educational and entertainment requirements.

Every user bears primary responsibility for the material he or she chooses to access, store, print, send, display or make available to others. The facilities may not be used in any manner to create, store, send, display or make available to others material which violates Library policy or any local, state or federal laws. When devices, such as portable computers, are the property of the user, the appropriate use expectations still apply when such devices are used to access the Library’s information technology facilities.

Failure to adhere to these guidelines may result in the suspension of access privileges as well as other action as deemed appropriate by the Library Director or Library Board of Trustees.

Appropriate use of information technology includes, for example:

* respect for the rights of others
* respect for the property of others
* consideration of other persons using shared systems, equipment and facilities
* confidentiality in use of passwords and personal identification numbers
* use of tools for the purpose for which they are intended
* adherence to the rules governing use of accounts, equipment, networks, or other facilities, whether the rules are established by the Library or by the organization providing these tools or services to the Library

Inappropriate use of information technology includes, for example:

* unauthorized access, alteration, destruction, removal and/or disclosure of data, information, equipment, software, or systems
* deliberate over-extension of the resources of a system or interference with the processing of a system
* disclosure of confidential passwords, personal identification numbers and/or access devices or information for accounts, equipment, and telephone voice mail
* propagation of hate literature
* propagation of pornographic materials
* harassment, including sexual harassment
* theft of resources
* malicious or unethical use, and
* use that violates local, state, and/or federal laws

***Position Statement on Censorship***

[Library name] does not and will not act as a censor of information available on our network, but will investigate properly identified allegations arising from employees and customers, and will comply with applicable local, state and federal laws. To the extent that the latter requires specifically identified information to be banned pursuant to a court order, [library name] will make every practical attempt to comply with both the spirit and the substance of the law.

**Guidelines Regarding the Issue of Potentially Offensive Materials**

These guidelines address the issue of potentially offensive information on the Library’s computer systems, whether generated locally or imported from other systems via the Internet. Any guidelines or procedures for handling this particular situation address only a single facet of a much broader policy issue regarding the production, storage, dissemination of and access to information available using information technology facilities. Rather than dealing with the global issue, these guidelines (in this section) focus only on handling, dissemination and display of objectionable material.

First, a guiding principle is the Library will ensure that its efforts to create an environment in which all its members treat each other with respect extend to facilities and activities associated with information technology.

There are wide variations in the range of things to which people take offense. What may be offensive to one person may seem innocuous or even informative to another. Generally, a person’s access to a particular piece of information will not be proscribed simply because someone else finds it offensive. On the other hand, no one should be involuntarily presented with information that the person transmitting it should reasonably know would be viewed by the recipient as offensive or insulting.

Thus, when an employee or customer, with properly authorized access to the Library network, actively seeks information that is legitimately and publicly available on a computer or network, the Library will ordinarily take no action to restrict that individual’s access based on the nature of the information being sought.

In situations where an employee or customer is presented, through the network, with offensive information without consent having been either sought or granted, the IT department will investigate the incident and take appropriate action. Such action may include, for example, referring any information about the incident to the Library Director, or assisting the complainant in bringing action under the appropriate Library policies or local, state or federal laws.

Complaints about potentially illegal information being produced locally will be investigated, and the Library may initiate criminal charges directly and/or actions under the relevant Library policies.

**Personal Privacy**

The property of the Library includes the facilities related to computing accounts and files and other aspects of the information technology network in a similar manner to the telephones, filing cabinets, desks, etc., which an employee uses in carrying out the duties of her or his job. In principle, they are subject to inspection at any time. In practice, however, such inspections other than for verification of physical assets are unusual and take place only where there is reason to suspect an infraction of the rules.

Under certain circumstances, access to files is authorized by Library policy, or, for example, library staff for the purpose of conducting the Library’s business may access certain customer files. However, if an infraction is suspected, the appropriate officials at the Library will investigate the matter and, if circumstances warrant, proceed to investigate the traffic and files associated with the suspected infraction in accordance with the applicable Library policy or procedure.

Such action requires the authorization of the Library Director. The IT Manager or Assistant Director for Operations should be advised promptly of any such action and be available to provide technical advice and guidance regarding suspected occurrences of inappropriate use.

It is essential that all users of information technology facilities and services recognize that it is possible for unauthorized individuals to monitor transmissions on networks in certain circumstances. It is also possible, for example, to create and send counterfeit mail under the name of another person and in a manner that makes it appear the message has emanated from the named user’s desktop. It is suggested, that confidential information not be sent electronically unless the user is operating on a known secure network or is using encryption mechanisms.

**Procedure in the Event of a Suspected Violation of Library Policy, Local, State or Federal Law**

The nature, severity and possible consequences arising from infractions of the use of Library’s information technology resources cover a wide spectrum. These can range from mere inconvenience or loss of privileges to damage of the Library’s reputation or even to charges being made if local, state or federal laws have been violated. The speed, nature and escalation of notification procedures should be commensurate with the severity of the infraction.

For infractions that contravene established Library policy or facility rules, the relevant local administrator should proceed in accordance with the applicable codes or rules, and should inform the IT Manager of the event and the action taken.

Violations that have broader consequences such as unauthorized access to and/or modification of data here or elsewhere, or the commission of illegal acts require additional consideration. The process should include notification of the IT Manager, Assistant Director for Operations and the Library Director

Should circumstances warrant it, the IT Manager and the Assistant Director for Operations will inform the Library Director before any decision is made to inform the appropriate legal body or law enforcement agency.