Policy Title: Acceptable Use Policy for Information Resources

Supersedes/Amends: ________________________________

Prepared by: Richard Lindstrom  
Issued/Revised: _1/23/2008_

Effective: __7_/ __01_/ __2008__

I. Introduction

Charles Drew University of Medicine and Science (the University) provides a wide variety of information resources to its faculty, staff, and students, as well as members of the community in order to facilitate the University’s mission of education, research, and service.

The computers, computing systems and networks provided by The University are a shared resource, which requires that all members of the community respect the rights of others, the integrity of the resources, and act responsibly. All existing laws (federal and state) and University regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct.

In addition to this policy, the codes of personal conduct and use of University facilities also apply to the use of information resources.

II. Scope

University information resources are owned or licensed by the Charles Drew University. Access to them is a privilege for members of the University Community, and carries the obligation of using them responsibly for University related activities. This Acceptable Use policy applies to all users of the University computing and network resources, as well as all electronic information licensed by the University, including software, journals, databases and books. It applies regardless of whether access is initiated from a device located on or off campus.

III. Policy Statement

It is the policy of the University that its information resources be used ethically and legally, in accord with applicable licenses and contracts, and according to their intended use in support of the University's mission. Any use that would impede teaching and research, or hinders the functioning of the University, violates an applicable license or contract, or damages community relations or relations with institutions with whom we share responsibility, is a violation of this policy.

Individuals using computing or network resources belonging to the University must act in a responsible manner, in compliance with law and University policies, and with respect for the rights of others using a shared resource. The right of free expression and academic inquiry is tempered by the rights of others to privacy, freedom from intimidation or harassment, protection of intellectual property, ownership of data, and security of information.

Although the University respects a diversity of perspectives and accordingly does not condone either censorship or the unauthorized inspection of electronic files, persons should be aware that the normal operation and maintenance of University Information Resources require the backup of data and records, the logging of activity and the monitoring of general usage patterns. IT staff members must respect and ensure

Page 1 of 3
the confidentiality and privacy of the data they observe or access during the course of performing their duties.

Consistent with the constraints of confidentiality, a University official with the appropriate investigative authority may inspect files stored on any University Information Resource or monitor usage when there is cause to believe that a law or a University policy has been violated, when there is need to defend a civil or criminal claim filed against the University, or in conjunction with a workplace misconduct investigation, or there is a legitimate concern about the safety or well-being of a member of the University community. Each person should be aware that their electronic records, files and communications may be subject to the University’s obligation to respond to subpoenas or other court orders, reasonable discovery requests, internal audits and requests for documents pursuant to applicable law. The appropriate due process and policies will be followed depending upon whether faculty, academic staff, classified staff or students are alleged to be involved.

IV. Acceptable Use Guidelines

1. **Respect.** All users of the University’s information resources are expected to respect the rights of others, including rights to privacy and safety, and to use these resources responsibly.

2. **Individual Responsibility.** Authorization to access University information resources is granted to each individual for his/her exclusive use. No one may use an authorization granted to someone else.

3. **Security.** Everyone is expected to maintain the confidentiality of their identification codes and passwords. Reasonable care should be taken to ensure that unauthorized users do not gain access to this information.

4. **Misrepresentation.** Persons may not misrepresent themselves to gain access to resources or information, nor misrepresent themselves for any electronic communication. Persons may not use or attempt to use access credentials that have not been assigned to them as individuals, or provided for their use as University employees or students.

5. **Malicious Activity.** Persons may not alter or intentionally or unreasonably damage, disrupt, impair or waste University information resources or equipment, nor interfere with another person’s authorized access to them. Persons may not use information resources to create a hostile environment, or intimidate or offend others, nor deprive others of their reasonable use of information resources.

6. **Commercial, Political and Non-University Activities.** Persons may not use University information resources to promote or solicit sales for any goods, services, unauthorized charities, or other contributions unless such use conforms to University rules and regulations or unless such efforts are on behalf of a student organization recognized by the University. University employees may not use University resources to solicit donations for a political campaign. Except for research collaborations, no one may use University information resources to promote or advance the interests of any for-profit non-University entity, group or organization for commercial purposes unless appropriately authorized.

7. **Incidental Personal Use.** Information resources are a part of day-to-day work for all members of the University community, and incidental personal use is accepted. However, activities of an extensive or recurring nature that do not serve University purposes should be limited, so as not to interfere with the operation of these shared resources.

8. **Violations of other laws.** Persons may not use University Information Resources in a manner that violates federal, state, regulations or laws, or University policies, including, but not limited to, copyright laws.

9. **Use of Commercial Software.** All persons using University-provided software or Information Resources must do so only in accord with the applicable license agreements. Persons may use software not on the University’s “Supported Software” list only if there is no adverse impact on University Information Resources and documentation of software ownership is kept and available at the site where the computer is normally located. The University does not provide technical support for software not on the “Supported Software” list.
IV. Consequences of Misuse and/or Non-Compliance

Violation of University rules governing appropriate use of Information Resources may result in loss of access privileges, University disciplinary action, and/or criminal prosecution. The appropriate due process and policies will be followed depending upon whether faculty, academic staff, classified staff or students are alleged to be involved.