


POLICY MANUAL

 <p>LOUISIANA DELTA COMMUNITY COLLEGE</p>		POLICY IT_101	
		Page 1 of 7	
		Last Revision Date: September 14, 2011	
		Effective Date: April 15, 2002	
Section		Subject	Title Computer Network/Internet/Information Resources Usage

Purpose

Computing resources at Louisiana Delta Community College are provided for the use of students, faculty and staff to help carry out the mission of the College. The College encourages and promotes uses of computing and network resources by the College community that support this mission. Computer systems/electronic information systems include all computer based hardware, and software owned by the College, any communications hardware and software provided by the College for the purpose of accessing its computers, any computer network governed in part or whole by the College. Louisiana Delta Community College generally provides users access to computer services such as electronic mail and the Internet 24-hours a day, seven days a week. (The College reserves the right to bring these services down for maintenance as needed.)

Because of the nature of some of this information, access to it must be limited. However, because of Delta's role as a state-supported educational institution, it is the College's obligation to make suitable information available to both its internal and external constituents. Because of these potential conflicting needs -- limiting access to information and making information widely available -- it is the obligation of faculty, staff and students to make use of computer and Internet resources responsibly, ethically and legally.

General Scope

The College Department of MIS/IT shall have final authority over all data processing systems, information technologies and networks associated with LDCC, including the authority to access, evaluate and/or suspend the operation of a data processing system or network associated with Louisiana Delta Community College.

LDCC Network/internet General Guidelines and Usage Policies

General Guidelines

1. The College Network is defined to include any and all computer-based communications facilities, which are owned or operated under the supervision of Louisiana Delta Community College.
2. The College Network is for use by authorized persons legitimately affiliated with LDCC, consistent with and in the course of their official work, study and/or research.
3. The LDCC Network Administrator or the Department Head of the MIS/IT must approve all physical connections/modifications to the College Network.
4. The LDCC Department head of the MIS/IT must approve any computer related hardware and software, before purchase. Any purchase requisition related to computer related hardware or software must first have the approval of the Department Head of the MIS/IT before purchase can be made.
5. Any wiring being installed by College personnel or by a contractor must follow current wiring standards. The Network Administrator or the Department Head of the MIS/IT will oversee all contract work on the network. Payment for such work will not be rendered until the Network Administrator or Department Head of MIS/IT approves the work.
6. Access to non default shares must be approved by the user's department head and if needed consent of the owner of that share.
7. Requests for new technology (i.e. new computers, printers or software) must come from the user's department head.

Usage Policies

The computers, lines, servers, wiring and all components of the system belong to the State of Louisiana and are paid for by the taxpayers. None are to be used to individually benefit an individual except in pursuit of his/her official business for the State.

Individual groups or projects within LDCC may adopt more restrictive network usage policies that apply to their sub-networks and personnel within their area.

Acceptable Uses:

1. Communication for professional development, to maintain current or to collaborate in research and education.
2. The publication of information via the Internet's World Wide Web (WWW), File Transfer Protocol (FTP), or similar techniques with proof of the Department of MIS/IT

3. Other administrative communications or activities in direct support of LDCC projects and missions.

Prohibited Uses include:

1. Use for personal or for-profit activities, such as a personal business.
2. Use by friends, family members, relatives, or others not officially affiliated with and authorized by the College. The LDCC networks, including its dial-in lines, are not available as a substitute for private Internet service providers.
3. Any use that is likely, or intended, to cause unauthorized network disruption, system failure or information loss.
4. Any use related to achieving, enabling or hiding unauthorized access to systems, software or information either within or outside LDCC.
5. Direct connection to a College device via an outside internet service provider (ISP).
6. Bypassing or building a conduit through the College firewall.
7. Any use which violates LDCC Administrative Policies.
8. Accessing or downloading any child pornography materials. Violation of these rules will result in immediate suspension from LDCC.
9. Accessing or downloading sexually explicit materials. The violation of these rules may result in disciplinary review. In such a review, the full range of disciplinary sanction is available including the loss of computer use privileges, dismissal from the College and/or legal action.
10. An individual's computer use privileges may be suspended immediately upon discovery of a possible violation of these policies.

Information resources usage policies

Any user of College information resources who is found to have purposely or recklessly violated any of the following policies will be subject to disciplinary action up to and including discharge, dismissal, expulsion and/or legal action.

Integrity of Information Resources

1. *Modification or Removal of Equipment:* Technology users, including faculty, students and staff, may not in anyway modify or remove computer or network equipment, software, or peripherals that are owned by the College without proper authorizations. Absolutely no modification may be made to any computer, or peripheral, or network device without the permission of the Department of MIS/IT.
2. *Encroachment on Access and Use:* Computer users must not encroach on others' appropriate access to, or use of, College computer or network devices. This includes but is not limited to: the sending of chain letters or excessive messages, either locally or off-campus; printing excess copies of documents, files, data or programs; running grossly inefficient programs when efficient alternatives are known by the user to be available; unauthorized modification of system facilities, operating systems or disk partitions; attempting to crash or tie up a College computer or network and damaging or vandalizing College property.
3. *Unauthorized or Destructive Programs:* Computer users must not intentionally develop or use programs which disrupt network or computer use, or which access private or restricted portions of a system and/or damage the software or hardware components of a system. Computer users must use great care to ensure that they do not use programs or utilities that interfere with other computer users or which modify normally protected or restricted portions of the system or user accounts. Computer users must not use network links for any use other than those permitted in the network guidelines.
4. *Academic Pursuits:* The College recognizes the value of research on computer security and the investigation of self-replicating code. The College may restrict such activities in order to protect College and individual computing environments, but in doing so will take into account legitimate academic pursuits.

Passwords

Use of passwords shall conform to the following requirements:

1. Passwords shall be kept confidential.
2. Twelve character minimum length and expire every 105 days.
3. Categories of password complexity shall contain at least 3 of the 4 categories: English upper case characters (A-Z), English lower case characters (a-z), Base 10 digits (0-9), and non-alphanumeric characters (e.g. %, &, !).
4. Passwords shall not be kept on paper or stored in plain text format.
5. All passwords shall be changed whenever it is determined that a system's security may have been compromised.
6. The cycling or re-use of passwords shall be reasonably limited. Applicable devices and application systems shall maintain a password history file to prevent continual re-use of the same passwords or group of passwords for a valid user-ID (with 3 being the minimum number of previous passwords checked).

Distribution Lists

We have set up the all@ladelta.edu list to include all Delta Employees.

Main Distribution Lists

all@ladelta.edu – MainCampus, Tallulah and Lake Providence

MainCampus@ladelta.edu – Emails employees at the Main Campus.

LakeProvidenceAll@ladelta.edu – Emails employees at the Margaret Surles Campus

TallulahAll@ladelta.edu – Emails employees at the Tallulah Campus

Adjuncts@ladelta.edu – Emails current adjuncts at all locations. These will not be sent an email using the all@ladelta.edu list.

These distribution lists are to be used for work related purposes or LA Delta sponsored events only. **They are not be used to promote events or fundraisers not associated with Delta.**

If a user sends an email to any large group, including these distribution lists, use the *Blind Carbon Copy* option in your email. This assures that any replies will be sent only to the sender and that if you are sending to external parties that you are not sharing any email addresses. To use the blind carbon copy option while composing your message click on the options tab and click on the "show bcc" icon.

Unauthorized Access

1. *Abuse of Computing Privileges:* Users of College information resources must not access computers, computer software, computer data or information or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information or network in question is owned by the College. For example, abuse of the networks to which the College belongs or the computers at other sites connected to those networks will be treated as an abuse of Louisiana Delta Community College computing privileges.
2. *Reporting Problems:* Any defects or abuse discovered in system accounting or system security must be reported to the appropriate system administrator so that steps can be taken to investigate and solve the problem.

3. *Password Protection*: A computer user who has been authorized to use a password-protected account may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the system owner.

Privacy

Computer users must respect the privacy of other computer users. Attempts to gain unauthorized access to the system or to private information are violations of College policy and may violate applicable law. Department administrators, with authorization from the Department Head of MIS/IT, may access computer users' files for critical maintenance purposes or in response to suspected policy violations. Department administrators will report suspected unlawful or improper activities to the Department Head of the MIS/IT. Any issue involving IT personnel will be handled in conjunction with the Human Resources department.

1. *Unlawful Messages*: Use of electronic communication facilities (such as mail or chat or systems with similar functions) to send fraudulent, harassing, obscene, threatening or other messages that are a violation of applicable federal, state, or other law or College policy is prohibited.
2. *Mailing Lists*: Users must respect the purpose and charters of computer mailing lists (including local or network newsgroups and bulletin boards). The user of an electronic mailing list is responsible for determining the purpose of the list before sending messages to or receiving messages from the list. Subscribers to an electronic mailing list will be viewed as having solicited any material delivered by the list as long as that material is consistent with the list's purpose. Persons sending to mailing list any materials that are not consistent with the list's purpose will be viewed as having sent unsolicited material.
3. *Advertisements/solicitations*: In general, the College's electronic communication facilities should not be used to transmit commercial or personal advertisements, solicitations or promotions (See Commercial Use, below).
4. *Information Belonging to Others*: Users must not intentionally seek or provide information on, obtain copies of or modify data files, programs or passwords belonging to other users without the permission of the other user and, where applicable, the permission of the Department administrator and Department head of the MIS/IT.
5. *Confidentiality*: The College does not exist in isolation from other communities and jurisdictions and their laws. Under some circumstances, as a result of investigations, subpoena or lawsuits, individual users or the College may be required by law to provide electronic or other records or information related to those records or relating to use of information resources.

Political, Personal, and Commercial Use

The College is a non-profit, tax-exempt State owned organization and, as such, is subject to specific federal, State and local laws regarding sources of income, use of real estate and similar matters. It is also a contractor with other governmental units and other entities and thus must

ensure proper use of property under its control and allocations of overhead and associated costs. Uses of the College's information resources, including the use of the College computer network capabilities, are, therefore, subject to the following conditions:

1. *Political Use:* College information resources must not be used for partisan political activities where prohibited by federal, State or other applicable laws, and may not be used for other political activities, except when in compliance with federal state and other laws and in compliance with applicable College policies.
2. *Personal Use:* College information resources may not be used for personal activities not related to College business and functions.

Commercial use: College information resources should not be used for commercial purposes except in a purely incidental manner or as permitted under other written policies of the College or with the written approval of a College officer having the authority to give such approval. Any such commercial use should be properly related to College activities, take into account proper cost allocations for government and other overhead determinations and provide for appropriate reimbursement to the College for other costs the College may incur by reason of the commercial use.