Internet Acceptable Use Policy

Revised: January 8, 2009

Read the following document carefully before accepting responsibilities of accessing a user account with the Licking Area Computer Association (LACA). This is a legally binding document.

GENERAL INFORMATION

The LACA communication network is an electronic computer network with access to the Internet. Our goal in providing this service is to promote educational excellence in school districts participating in LACA by facilitating resource sharing, innovation, and communication. Through participation in this effort, LACA provides to the Licking, Muskingum, and Knox County communities a network offering vast, diverse, and unique resources. As used in this Policy, "network" refers to interconnected computer systems, computer equipment, computer programs, the Internet, electronic mail, IP- or Internet-based telephone systems, and related communication technologies.

Along with access to computers and people all over the world comes the availability of material which may not be considered to be of educational value within the context of the school setting. LACA and the OECN firmly believe the valuable information and interaction available on this worldwide network far outweigh the possibility users may procure material inconsistent with educational goals for the district or network.

Internet access is coordinated through a complex association of government agencies, regional, and state networks. The smooth operation of the network relies upon the proper conduct of the end-users, who must adhere to strict guidelines. These guidelines are provided here so the user is aware of the responsibilities associated with use of this network.

In general, network use requires efficient, ethical, and legal utilization of the network resources. If any users violate any of these provisions, their current and future access of the LACA network could be denied. The signatures on the Internet Application and User Agreement Form for Use of the LACA Network are legally binding and indicate the parties who signed have read the terms and conditions carefully and understand their significance.

GENERAL NETWORK USE GUIDELINES

Use of the LACA network is a privilege, not a right. Inappropriate use will result in a cancellation of privileges. LACA system administrators, in conjunction with district administrators, will deem what is inappropriate use of the network; their

decision is final. The system and district administrators may terminate a user's ability to access the LACA network at any time as required. If a specific user account has been issued, the administration, faculty, and staff of LACA's contracted districts may request the system administrators to deny, revoke, or suspend specific user accounts. The following guidelines should be used to determine eligibility for the granting of access to the LACA network:

Eligibility

1. All district personnel who are contracted users of LACA and the OECN, including, but not limited to, prekindergarten-grade twelve educators, support personnel, administrators, school specialists, and county offices of education staff members.

2. All prekindergarten-grade twelve students whose district is a contracted user of LACA and the OECN when under the supervision of a sponsoring educator. Student access will expire at the end of each regular school year or upon the student withdrawing from the district.

3. Network resources are only for use by authorized users. Authorized users must not share their passwords or otherwise allow anyone to gain unauthorized access to the Network or the Internet. Anonymous accessing of the Internet only for legitimate educational or administrative purposes is permitted if authorized by the user entity, subject to any reasonable security measures which may be implemented by the user entity. LACA shall not be responsible for any inappropriate online activities of persons making use of the system pursuant to a user entity policy allowing Internet-only access on an anonymous basis.

4. Acceptance of the terms of this Internet Acceptable Use Policy is required in order to be an authorized user.

5. LACA system administrators reserve the right to make the final determination on all issues relating to eligibility.

Security

Security on any computer network is a high priority, especially when the network involves many users. Individuals identifying a security problem on the LACA or OECN network have the obligation to notify the system administrators at the earliest possible time. The problem should be reported via telephone, if possible, or E-mail if the user is reasonably sure E-mail is secure.

A copy of the LACA Data System Security Policy is attached to and considered a part of this Agreement. Attempts to logon to the LACA

system without an account or as any other user will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access.

Purpose

The purpose of the Internet within the school setting is to support research and education in and among academic institutions in the U.S. by providing access to unique resources and the opportunity for collaborative work. Use of other organization's networks or computing resources must comply with rules appropriate for that network. User access must support goals consistent with the educational objectives of LACA member school districts. Listed below are the acceptable and unacceptable uses of the LACA network.

ACCEPTABLE USES OF THE LACA NETWORK

1. Communication with foreign researchers and educators in connection with research or instruction, as long as any network that the foreign user employs for such communication provides reciprocal access to US researchers and educators.

2. Communication and exchange for professional development, to maintain currency, or to debate issues in a field or subfield of knowledge.

3. Use for disciplinary-society, university-association, government-advisory or standards activities related to the user's research and instructional activities.

4. Use in applying for or administering grants or contracts for research or instruction, but not for other fundraising or public relations activities.

5. Any other administrative communications or activities in direct support of research and instruction.

6. Announcements of new products or services for use in research or instruction but not commercial advertising of any kind.

7. Any traffic originating from a network of another member agency of the Federal Networking Council if the traffic meets the acceptable use policy of that agency.

8. Incidental personal use of the system to communicate with family, friends, and colleagues may be permitted as a convenience to employees provided such usage is limited in scope and is otherwise in compliance with this Policy and local school policies. Local school policies may modify or further define the scope of incidental personal use which may be permitted.

UNACCEPTABLE USES OF THE LACA NETWORK

1. Transmission of any material in violation of any US or state regulation is prohibited. This includes, but is not limited to, copyrighted material; threatening or obscene material; or material protected by trade secret.

2. At no time may the network, the Internet, or IP- or Internet-based phone systems be accessed for purposes of engaging in any kind of business or other profit-making activity.

3. Users shall not use the Network in any way that would disrupt the operation of the Network; abuse the software and/or hardware; or cause the unnecessary use of system resources, including but not limited to mass mailings unrelated to school business, installing unauthorized software or games, sending spam, or chain letters, or making personal use of printer paper or disks.

4. Users may not move, repair, reconfigure, modify or attach any external devices to LACA provided Network equipment, without authorization.

5. Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to alter, destroy, or reduce the usability of data of another user, agency, or network connected to LACA, the OECN, or the Internet backbone. This includes, but is not limited to, the uploading or creation of computer viruses, worms, Trojan horses, etc.

DISCLAIMER

LACA, the participating districts and the OECN make no warranties of any kind, expressed or implied, for the service being provided and will not be responsible for any damages suffered, including loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by negligence, errors or omissions. LACA, the participating districts and the OECN specifically deny any responsibility for the accuracy or quality of information obtained through the network services; use of any such information is at the user's risk.

NETWORK RULES

The network is a public medium, and all users are expected to abide by the rules of network etiquette, including (but not limited to) the following:

1. No use of abusive language in messages;
2. No use of vulgarities, obscenities, or other inappropriate language/material, including reposting or quoting obscene and/or inappropriate language/material;

3. No revelation of personal addresses or phone numbers or system network passwords;
4. No reposting of private communications without prior consent of the author; all communications and information accessible via the network should be assumed to be private property; and
5. No use of the network which disrupts other users or seriously degrades performance of others: the network is a shared resource with finite capacities.
6. Avoid excess use of system resources by deleting electronic mail on a daily basis and canceling subscriptions to mailing lists for which there is no longer interest or prior to access termination.

Electronic mail (E-mail) is not guaranteed to be private; system administrators and operators have the right to access mail, and mail software may misdirect messages. Messages relating to or in support of illegal activities will be reported to appropriate authorities. Illegal activities of any nature are strictly forbidden and will be reported to the appropriate authorities. Violators will lose privileges to use the network and may face possible prosecution.

CONTINUED USE OF THE NETWORK

LACA may occasionally require new registration and/or account information from all or selected users in order to continue service. Users agree to notify LACA of any changes in account information (address, etc.) as soon as possible.

LACA NETWORK ADMINISTRATION

LACA system administrators reserve the right to limit or suspend access to the OECN and/or Internet or to supersede portions of this Agreement as may be deemed necessary for the maintenance, safety, or security of the LACA member districts or the OECN. The policy on network administration is listed below.

1. LACA reserves the right to suspend network access at any time to maintain the integrity of the network.
2. LACA reserves the right to suspend network access by a contracted district not complying with the Internet Acceptable Use Policy and the Data System Security Policy for use of the LACA Network. All decisions of LACA are final.
3. LACA reserves the right to suspend access temporarily or permanently to any user who does not comply with the Internet Acceptable Use Policy and the Data System Security Policy for use of the LACA Network or for any reason deemed appropriate by the system administrators to maintain the integrity of the network. All decisions of LACA are final.
4. LACA reserves the right to recommend criminal charges against any user who does not obey applicable state and federal laws.
5. LACA reserves the right to log Internet use and to monitor network and system resources utilized by the user while respecting the privacy of the user.

6. LACA reserves the right to monitor user accounts for system administration while respecting the privacy of user accounts.

7. LACA reserves the right to modify this policy upon Governing Board approval and 30-days' notice to authorized users and user entities. All users and user entities will be deemed to have accepted such modifications unless written refusal is delivered to LACA within such 30-day period. Refusal to accept the terms of this Internet Acceptable Use Policy shall result in the loss of eligibility for network and Internet access.

8. LACA firmly believes in the rights and guarantees provided by the laws of the state of Ohio and the United States of America. No intentional violation of these rights will occur.

LACA Data Security Policy

Approved: January 8, 2009

The Governing Board and staff of the Licking Area Computer Association (hereafter referred to as the Computer Center) recognizes that data maintained by the Computer Center is the legal property of the school district (hereafter referred to as the district) which entered such data or to which such data is assigned. Each district's individual portion of the Computer Center's computer which maintains district data is considered an extension of the district. The Computer Center, therefore, is a holder in public trust of the data.

The Board adopts the following policy statements concerning access to and security of the data. These statements are intending to assure the inviolability of the data, provide for procedures to permit authorized access to data and prohibit unauthorized release of data, and recommend features which districts and the Computer Center can implement to promote system and data security.

I. DATA ACCESS

Data maintained by the Computer Center shall be recognized as the exclusive property of the district. Each district shall be in control of its own data maintained by the Computer Center. Access to the data shall be granted as follows:

A. DISTRICT PERSONNEL

1. District personnel shall be granted access upon the authorization of the District's Superintendent and Treasurer.

2. Such access may be restricted (as may be practical or technically possible) to certain data files and/or specific access types.

3. The Computer Center shall provide an electronic method for authorization.

4. District personnel shall exercise caution when accessing sensitive data which may include student or employee personal information, from outside the LACA or District network. Computers and browsers can cache temporary copies of the files that are accessed, potentially exposing the District and personnel to liabilities.

B. COMPUTER CENTER PERSONNEL

1. Computer Center staff shall be granted access when such access is within the scope of their assigned duties, but only as may be necessary to maintain the data structure, research and correct problems, and provide backup capabilities.

C. OUTSIDE ACCESS

1. Outside access shall be granted upon the written authorization from the Superintendent of the district or his/her designee.

   a. "Outside" is defined as any individual or group of individuals not belonging to the school district or the Computer Center.

2. Data required to be transferred to the Ohio Department of Education shall be as defined by statue, State Board of Education Rule, and/or as outlined in the "Education Management Information System: Definitions, Procedures, and Guidelines."

3. Written confirmation of the outside access shall be forwarded to the district superintendent within 24 hours.

II. DATA SECURITY PROCEDURES

The first point of security is access to the computer system and its data via the local network of users. To enhance security and reduce the risk of unauthorized access, the following guidelines shall be followed:

A. Users will be assigned one unique log on for access to all authorized systems.

B. Each user account shall require a password with a minimum of 6 characters. This password shall be treated as confidential information by the user. Users are responsible to safeguard their passwords, other access protocols, and district and Computer Center information, in whatever form. No list of passwords shall be maintained by the Computer Center or the District.

C. All interactive user's passwords will automatically expire every 90 days. All interactive users will be held captive to the MENU system.

D. Users should ensure their terminals, when not in use, are properly logged off the system.

E. Users shall be granted only those privileges consistent with the duties and responsibilities of their position. Authorized privileges shall be grouped in a "normal" and "extended" category: "normal" privileges are granted by the system when a user logs onto the system and represent the privileges required to perform the user's normal duties; "extended" privileges are those privileges which the user may be authorized to use, but which must be specifically enabled for the user by the Computer Center before being utilized.

F. Users shall take every precaution to safeguard sensitive information by not saving or downloading such information from LACA's systems to unsecure devices. Examples of such devices are mobile phones/devices, laptops, USB drives, floppy disks, CDs or DVDs, public computers (libraries, etc), or employee owned computers.

G. Users granted elevated access to information may find they have access to information above and beyond what is needed to perform their job duties due to limitations in software security

capabilities. In these cases, users will refrain from accessing any information that is not relevant to their job functions.

H. Access to the computer system via an electronic network outside the Computer Center area will be restricted to the minimum level of access necessary for authorized users.

I. Access to privileged or system accounts shall only occur with the authorization of the Computer Center Director. Following outside access to a privileged account, the account password shall be changed to prevent further access without the Computer Center staff's knowledge.

J. AUDIT LOG

Sufficient audit alarms shall be enabled to track attempts to break into a users or system account and other security related events. The audit log shall be reviewed weekly for suspicious entries.

K. NOTIFICATION BY DISTRICT USERS

1. For security reasons, each district should immediately notify the Computer Center if an employee has been terminated or has left the district. The accounts and files of the employees shall be disabled immediately and deleted within five business days.

2. Each district should notify the Computer Center when any district user is placed on leave of absence, or short-term or long-term disability. The user's account shall be completely disabled and re-opened only at the request of the user's immediate supervisor. The District shall also submit their user paper and/or electronic security form noting the dates involved for the leave.

L. In all events, the Director of Computer Services shall have the authority and responsibility to take actions necessary to insure the integrity of the data and security of the computer system, or to enable authorized district users to utilize the computer system to fulfill the duties associated with their positions.

M. The data security policy and procedures shall be reviewed annually.

III. DATA STORAGE AND RECOVERY

LACA generates and maintains back up copies of E-mail data for 7 days, of SQL data for 14 days and all other data for 30 days. Point-in-time restores from specific days may not always be possible. Incremental back-ups are created nightly. Back-up copies are rotated to the off-site location on a daily basis. These back-ups include all data and applications stored on LACA's servers and SAN (storage area network).

LACA will restore data from a given point in time when requested by an authorized district representative. LACA reserves the right to request permission from district staff with higher authority before performing any data restoration, depending on the nature of the data to be restored, or the requestor's level of authority. Retrieving data for daily school district operations will be a top priority.