7:390 Technology Acceptable Use Policy/Password Policy and Guidelines

TECHNOLOGY ACCEPTABLE USE POLICY

Lockport Township High School District 205 provides technology for use as a tool to enhance classroom teaching and learning. Access to the computer Network and the Internet offers valuable, diverse, and unique resources to users. The appropriate use of technology promotes educational excellence by facilitating resource sharing, innovation, and communication.

Curriculum

It is the mission of the District 205 educational community to provide a curriculum for its students which is dynamic, engaging, and sensitive to the continually changing needs of a global society. To that end, the District 205 educational community is committed to providing the necessary technological tools and instruction which will maximize each user's ability to acquire, retrieve, construct, and present information. The use of the District 205 computer Network and Internet resources shall be consistent with the curriculum objectives adopted by the district as well as the varied instructional needs, learning styles, abilities, and developmental levels of its students. The Internet and District 205's computer Network are part of the District's curriculum and not a public forum for general use.

Privilege Statement

The use of Lockport Township High School's computer Network and connections to the Internet is a privilege, not a right, and inappropriate use as defined by Board Policy will result in cancellation of the privilege. Improper or prohibited use of the District computer Network may also result in the imposition of disciplinary measures as defined by the District's disciplinary code.

Monitoring of User Accounts

Lockport Township High School intends to monitor use of its Network including, but not limited to, e-mail, Internet access, downloaded materials, storage media, printing, and other general activity. Accordingly, District staff may review files and messages created or viewed by users at any time. Although staff members will monitor and promote proper use of the Internet/Network, it is the responsibility of each person to use the Internet/Network in a responsible and appropriate manner and the District specifically disclaims liability for any harm caused by misuse of the Internet/Network or from any materials or information obtained from the Internet/Network.

Acceptable Use

The purpose of using computer technology is to support research and education that promotes the values and objectives of this community of learners. All use of the Network must be consistent with the purpose and in accordance with this policy. The District's authorization for internet access is a privilege that requires each user to adhere to the responsibility of acceptable use. This Policy does not attempt to state all required and prescribed behavior by users, however, some examples are provided:

1. Acceptable Use - Access and use of the school district's computers must be in accordance with the mission of Lockport Township High School District 205 and promote the purpose of education or research. The District system may not be used for any unlawful activity or for any commercial activities. The following general guidelines are noted. Acceptable Use Guidelines:

    a. Be responsible for hardware and software equipment (i.e. notify your teacher of any change in the condition of equipment).

    b. All communication must be respectful of others.

    c. For your safety, do not reveal any personal information about yourself or others.

    d. At all times you are expected to be polite and considerate.

2. Network Etiquette - You are expected to abide by the general rules of decency; which include, but are not limited to the following:

    a. Avoid using offensive, provocative or vulgar language.

    b. Do not misrepresent yourself or others on the Network.

c. Recognize that electronic mail and other correspondence is not necessarily private. And remember that school staff may review and access your messages at any time.

d. Never engage in any illegal activities.

3. Users are not to engage in any form of:

a. "Hacking" (unauthorized probing) and/or "Cracking" (making unauthorized changes); bypassing the Internet filtering proxy, using proxy avoidance sites.

b. Downloading of copyrighted material or making unauthorized copies of software found on District computers or otherwise violating any license agreement; accessing inappropriate or unauthorized areas.

c. Wasting physical and/or electronic resources.

d. Sending anonymous messages.

e. Introducing a "virus" to the system.

f. Using the district technology for personal (financial) gain.

g. Transmitting or accessing any obscene, lewd, lascivious or pornographic material.

4. Access to Network resource:- Each person is given an individual user ID and password to logon to school Network resource:

a. DO NOT share your school user ID or password to others.

b. Do not use your school user ID and password to gain access to unauthorized school resources.

c. Never use another person's user ID and password at anytime.

d. If you are unable to access resources with your school user ID and password please ask a staff member for help.

5. Network data drives:- Users will be given an Network drive to save and store school classroom related work only:

a. DO NOT share your data with other users.

b. Network storage should contain school related material only.

c. Network storage should not contain illegal or copyrighted material.

Unacceptable Use

You, the user of district resources, are expected to be responsible for your actions. Misuse of the equipment or the Network will result in consequences that may include denial of user privilege, suspension or even expulsion from school, and restitution. In situations where a negligent act has caused a loss to the District, the perpetrator will be expected to make restitution for the damages or be responsible for reimbursing the District as a result of the unauthorized use or misuse. When in doubt about any particular action, the user is expected to ask the teacher for advice.

Computer and Internet/Network users are expected to follow the direction of their instructor and conform to the educational purpose of the technological equipment. Inappropriate conduct will be referred to the dean of students or the administration for assessment and possible disciplinary action. The system administrator, in conjunction with the administration may investigate incidences of unacceptable use. Users will be held accountable for their misuse of the system and equipment.

No Warranties

Lockport Township School District 205 makes no warranties of any kind, whether expressed or implied, for the service it is providing. The district will not be responsible for any damages users may suffer. These damages include loss of data resulting from delays, non-deliveries, missed-deliveries, service interruptions or errors and/or omissions caused by the negligence of user. Use of any information obtained via the Internet/Network is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained by Internet/Network users.

Restitution

The user agrees to make compensation to Lockport Township School District 205 for any losses, costs, or damages, including reasonable attorney fees incurred by the District relating to, or arising out of any breach of this policy and/or procedures. The user will also be responsible for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, fines for breech of license, and/or equipment or line costs.

Security

The Internet/Network security is essential for the user to maintain. If the user can identify a security problem on the Internet/Network, the user must notify the teacher and/or the Network administrator. The security problem is not to be divulged or demonstrated to any other user. The user is to keep his/her account and password confidential. Another user's account and password is not to be used for any reason or at any time. Attempts to log-on to the Internet/Network as a Network administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the Internet/Network.

Vandalism

Vandalism will result in cancellation of privileges and other disciplinary action as prescribed in this policy and the Student Handbook. Vandalism is defined as any malicious attempt (physical or electronic) to harm or destroy hardware, software, or data of another user, the Internet, or any other Network. This includes, but is not limited to, the downloading, uploading or creation of computer viruses.

Disciplinary Action

Individuals who violate this policy may be subject to one or all of the following consequences:

1. Reimbursement to the District by the offender for costs incurred by the District to return the computer equipment, programs, files, telecommunication Network and room environment to full operating condition.
2. Access to Network resources may be limited, suspended, or revoked (without notice to user).
3. Detention or Suspension.
4. Recommendation for an expulsion hearing.
5. Notification to the appropriate law enforcement agency.

Termination of Authorization

The guidelines of this policy are provided so that you are aware of your responsibilities. In general this requires efficient, ethical, and legal utilization of the Network resources. If an individual in Lockport Township High School District 205 violates any of these provisions, disciplinary consequences as set forth and described in this document may be applied.

User Statement of Understanding

I understand and will abide by the above policy for school Network and Internet access. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. I am also aware that should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or appropriate legal action may be taken. In consideration for using the District's Network and Internet connection and having access to public Networks, I hereby release the School District and its Board Members, employees, and agents from any claims and damages from my use, or inability to use the school Network and Internet.

Last Name: _____ First Name: _____

ID #: _____ Year of Graduation: _____

_____ _____

Student Signature Date

Parent/Guardian Statement of Understanding

I have read this Policy for the school Network and Internet access. I accept financial responsibility for the

actions of my child and agree to compensate Lockport Township High School District 205 for any losses, costs, or damages, including reasonable attorney fees incurred by the District relating to, or arising out of any breach of this policy and/or procedures by my child. I understand that access is designed for educational purposes and that Lockport Township High School District 205 has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by materials or software obtained via the Network or Internet. I accept full responsibility for supervision if and when my child's use is not in a school setting. I have discussed the terms of this Policy with my child. I hereby request that my child be allowed access to the school Network and the Internet.

_____ _____

Parent Signature Date

**********For School Use Only**********

Username: _____

Date of account creation: _____

By Sysop: _____

User Statement of Understanding

I understand and will abide by the above policy for school Network and Internet access. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. I am also aware that should I commit any violation, my access privileges may be revoked, and school disciplinary action and/or appropriate legal action may be taken. In consideration for using the District's Network and Internet connection and having access to public Networks, I hereby release the School District and its Board Members, employees, and agents from any claims and damages from my use, or inability to use the school Network and Internet.

I accept financial responsibility for my actions and agree to compensate Lockport Township High School District 205 for any losses, costs, or damages, including reasonable attorney fees incurred by the District relating to, or arising out of any breach of this policy and/or procedures. I understand that access is designed for educational purposes and that Lockport Township High School District 205 has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial and inappropriate materials. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by materials or software obtained via the Network or Internet. I hereby request that I be allowed access to the school Network and the Internet.

Last Name: _____

First Name: _____ Job Title: _____

Department: _____ Extension: _____

**********For School Use Only**********

Username: _____

Date of account creation: _____

By Sysop: _____

Personnel

PASSWORD POLICY AND GUIDELINES

Last Revised: 10/23/06

Purpose: To provide a policy for safeguarding access to the Lockport network through the creation of strong passwords and ensuring accountability for password protection, and to provide guidelines and techniques for creating strong passwords.

Policy: Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of LTHS's entire network. As such, all LTHS's network users (including LTHS's employees, contractors, vendors, and non- LTHS's persons with access to LTHS's systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their own individual passwords.

Exceptions: There are no exceptions to this policy.

Policy: Automatic Strong Password Structure Will be Enforced.

1. **Enforce password history:** **(24)** determines the number of unique new passwords a user must use before an old password can be reused.

2. **Maximum password age:** **(75)** determines how many days a password can be used before the user is required to change it.

3. **Minimum password age:** **(2)** determines how many days a new password must be kept before the user can change it.

4. **Minimum password length:** **(6)** determines the minimum number of characters a password can have.

Passwords must meet complexity requirements: user passwords must meet the following requirements: **-** The password is at least six characters long. - The password does not contain three or more characters from the user's account name. **-** The password must contain one uppercase letter, one number, and one lower case letter.

Guideline: Highly Recommended Strong Password Criteria

1. Passwords should not be words in any language, slang, dialect, jargon, etc.

2. Passwords should not be based on personal information, family names, etc.

3. Passwords should never be shared, written down, or stored on-line.

Guideline: Techniques for Strong Password Creation

4. One technique for creating a strong password is to create an acronym password based on a song, affirmation, or phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

5. Another technique is to use a phrase with some slight variation. For example, the phrase might be: "Happy New Year" and the password could be "HappY_nEw yeAr"

NOTE: You can use spaces, however, they do not count as a characteristic for creating a strong password.

Guideline: Poor or Weak Password Characteristics

6. Contains less than eight characters.

7. Is a word found in a dictionary (English or foreign).

8. Is a common usage word such as:

- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms, commands, sites, companies, hardware, software.
- Words such as LTHS, Lockport, Porters, or Wildcats.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Guideline: Password Protection

9. All passwords are to be treated as sensitive, confidential FSO information. Do not share passwords with anyone, including supervisors, bosses, administrative assistants, secretaries, co-workers, or groups.

1. Do not reveal a password over the phone to ANYONE.
2. Do not reveal a password in an email message.
3. Do not reveal a password to the boss.
4. Do not talk about a password in front of others.
5. Do not hint at the format of a password (e.g., "my family name").
6. Do not reveal a password on questionnaires or security forms.
7. Do not share a password with family members.
8. Do not reveal a password to co-workers while on vacation.
9. Do not write passwords down and store them anywhere in your office.

Do not store passwords in a file on ANY computer system without encryption (including Palm Pilots or similar devices).

CROSS REF.: 5:340 (Student - Acceptable Use Policy/Password Policy and Guidelines)

ADOPTED: August 20, 2007