Technology Code of Conduct

The LISD promotes and encourages the use of a wide variety of technology applications in education. Although the benefits associated with technology are great, there also exists the potential for misuse which can be both distracting and harmful. In order to promote the responsible use of technology, the LISD requires that all persons using LISD technology must have proper authorization for the specific legitimate educational use or school business intended, and must adhere to the LISD's Technology Acceptable Use Policy and related administrative procedures.

In order to ensure that all users of LISD provided technology applications are aware of the responsibilities associated with the use of District provided technology, new users will be prompted to review and accept the District's Technology Acceptable Use Policy. By accepting the provisions of the District's Acceptable Use Policy, technology users affirmatively agree that they have read, understood, and agreed to comply with the Policy. Failure to comply with the provisions of the Technology Acceptable Use Policy may result in termination of a user's ability to use District technology, as well as other disciplinary measures as determined by the school administration. Furthermore, the District reserves the right to inform the appropriate law enforcement agency if misuse violates local, state, or federal law.

The LISD reserves the right to monitor and review individual use of LISD technology. User activities on LISD technology may be monitored and logged.

LISD TECHNOLOGY ACCEPTABLE USE POLICY

I. APPLICATION:

The Lenawee Intermediate School District's (LISD) information systems network is intended for legitimate school business and educational purposes only. The Technology Acceptable Use Policy shall apply to all users of the Lenawee Intermediate School District's educational technology resources including LISD equipment used offsite and personal equipment used onsite. Violation of the Technology Acceptable Use Policy may lead to disciplinary sanctions, depending on the circumstances, and the severity and frequency of the infraction(s), including, but not limited to: reprimand (verbal and/or written), seizure and confiscation of personal property involved in the infraction, search, detention, suspension, expulsion, future restrictions or limits on access to such technology, filing of criminal charges, or termination of employment.

II. DEFINITIONS:

1. Educational Technology: in the context of the District's Mission, any method, material, process, equipment, etc. that is part of a system for providing desired learning outcomes as specified in the Michigan Educational Technology Standards (METS). Equipment includes but is not limited to, computers, disk drives, printers, scanners, networks, video and audio recorders, cameras, photocopiers, facsimile machines,

telephones, modems, external or removable storage devices, cell phones, pagers, webcams, mobile devices, wireless devices, and other related electronic resources.

2. User: any person that uses the District's technology in learning or in the support of the organization and its partners, including but not limited to, Board of Education member, school executive, administrator, teacher, assistant, bus driver, Secretary, employee, staff, students, contractor, member, party to an access agreement, and guests.

3. Technology Acceptable Use Policy: a set of policies, standards, rules, regulations, privileges and responsibilities governing activities and related matters, and applied to all users of the District's educational technologies.

4. Internet: a global network of computers and information systems, usually accessed by remote users for the purpose of electronic communications between users and/or devices. This term includes "links" that connect users to computers and information systems all over the world.

5. Local Area Network: a local area network (LAN) is a configuration of more than one personal computer, one or more file or application servers, and related devices, including but not limited to, scanners, printers, modems, cabling and connections, routers, webcams, mobile devices, hubs, repeaters, disk storage arrays, CD-ROM drives, fax servers, and input devices, directly physically or electronically connected together for the purpose of electronic communications between users and/or devices.

6. Wide Area Network: more than one LAN, including wireless services available on district property, usually located in different places (buildings, districts, towns, counties, etc.), connected together electronically, including but not limited to, telecommunications services, dedicated cables, fiber optics, microwave or other radio signals, etc., for the purpose of electronic communications between users and/or devices.

III. USER PRIVILEGES:
LISD users have certain privileges when in school and while using the District's technology resources.

A. Access Privileges: A user's privilege to access educational technology resources may be restricted, suspended, or revoked for violation of these policies. Access may also be inhibited by certain actions, including but not limited to routine maintenance, device availability, daily schedules, course requirements, safety concerns, and assignments and reassignments.

B. Freedom of Speech: The First Amendment rights of citizens, under the United States Constitution and its amendments, shall apply to users of educational technology resources, except where limited for pedagogical purposes or other legally recognized limitations (abuse, obscenity, defamation, etc.).

C. Property Rights: Users have ownership rights over their own intellectual property produced, created, or copied on the District's educational technology resources, unless the "work-for-hire" doctrine applies to employees and contractors (works prepared by an employee within the scope of his or her employment, or a work specially ordered or commissioned and expressly understood to be a work for hire), as provided in the District's Policy on Copyright Protection.

IV. USER RESPONSIBILITIES:

With privileges come responsibilities. Each user is to be held accountable for his/her actions as it relates to the use of technology resources accessible through his/her position with the LISD. Awareness and knowledge of the appropriate use of technology resources is important in order to maintain compliance.

A. Proper Authorization: To ensure that users may take full appropriate advantage of the educational technologies available in the District, all use of technology must have proper authorization. The source of proper authorization will depend upon the user's status in the District. Students must have permission for the specific use from their teacher; staff must have permission from their supervisor; administrators should have permission from their supervisor, or such use must fit within their general job responsibilities

The means for documenting proper authorization shall be determined, depending upon the user's role and other circumstances, within the discretion of school officials responsible for providing access to such educational technology to users.

B. Type of Use: Use of the District's technology is limited to legitimate educational purposes which enhance the school curriculum and/or school business operations and/or which are consistent with the District's mission statement. The following uses are strictly prohibited and may subject the offender to restriction, suspension or termination of educational technology privileges, and to appropriate disciplinary sanctions, such conduct to include but not be limited to:

- unauthorized entry into a file, whether to use, read, change or for any other purpose;
- unauthorized transfer, deletion, or duplication of a file;
- unauthorized use of another individual's identification or password;
- unauthorized access to computer or network equipment, facilities, and scanning for system vulnerabilities;
- use of technology equipment which interferes with the work of another student, faculty member, or school official (i.e. streaming music or video;
- instant messaging; gaming);
- intentional use of a proxy to circumvent LISD internet filtering mechanisms;
- use of personal or district technology to draft, send, or receive inappropriate communications (i.e. any picture, graphic, text, or audio file) including, but not limited to, communications which are indecent, obscene, pornographic and/or

sexually explicit, profane, vulgar, threatening, bullying, defamatory or otherwise prohibited by law;
- use of applications on the LISD “Do Not Install” List;
- use of district or personal technology to interfere with the operation of the LISD’s computer systems (i.e. downloading, uploading and/or executing of malicious coding or unauthorized altering of setup preferences, programs, properties or other system settings);
- violation of copyright, trademark, trade secrets, or licensing agreements (i.e. installing a second copy of a single licensed software);
- use of computing equipment for the purchase, sale, and/or advertisement of goods and services other than those directly operated or offered by the Board of Education and the District.

C. User Initiative: Users are responsible for attending appropriate training sessions in the use and care of educational technology and should refrain from using any technology for which they have not received training unless supervisor-approved self-teaching is necessary or desired. Users may be required to make full or partial financial restitution for any damages to educational technology or unauthorized expenses incurred through the use of educational technology. Users are encouraged to report security problems in a prompt fashion and to the proper authorities.

D. Identification and Password Integrity: Users shall maintain the integrity of their identification and passwords for using the District’s educational technology. Only authorized individuals shall routinely have access to user identification and passwords.

E. Computer Virus Protection: Users are expected to use the District’s computer technology in a manner that minimizes the risk of computer virus infection. Proper use of authorized protective anti-viral, spyware, and malware software is expected before any placement of executable files on the district’s storage devices.

F. Non-School District Owned Educational Technology Resources: When users utilize non-school District owned educational technology resources in the course of their school business, instruction, research, or other related activity, the user will be expected to abide by this policy as if the educational technology resources were owned by the District. For example, if a teacher brings a personal video camera to school to be used in conjunction with course instruction, school officials would expect that teacher to use the video camera in a manner consistent with this policy. Software owned or possessed by a user shall not be installed on the District’s computer hardware without the permission of the program supervisor and assurance that installation is compliant with the software’s licensing agreement. Such software must be removed from the computer upon the program supervisor’s request.

G. Respect for Others: It shall be each user’s responsibility to recognize and honor the rights, including intellectual property and privacy rights, of others in the use of educational technology resources.

H. Other Board Policies: Student users and parent(s)/guardian(s) of minor students may be required to execute a “Student Use and Parent Participation Form” acknowledging receipt of this policy and administrative procedures. Program administrators, in consultation with instructional staff, shall determine when to use the form. The users must adhere to other Board of Education policies in their use of educational technology. These policies include but are not limited to: anti-discrimination and sexual harassment policies intended to enhance equal educational opportunities to the diverse populations in our community, the Student Code of Conduct, Community and Staff Use of School Facilities, Drug-Free Workplace, the Code of Ethical Relationships, Smoking on School Premises, Off-Air Taping, Access to Financial Data, Access to Student Records, and other pertinent policies. Violations of such policies may subject the user to appropriate disciplinary sanctions.

V. INSTITUTIONAL RIGHTS AND RESPONSIBILITIES:

A. Contracts/User Agreements: The District shall make this policy governing use of educational technology resources a provision in its contracts concerning educational technology with other entities and users whenever feasible.

B. Response to Inappropriate Materials: District officials shall take measures to reduce the incidence of access to inappropriate materials using the District’s educational technology resources, via the following means:

- catalog and block offensive providers;
- maintain an extensive log of all user activities;
- require user identification and passwords where possible;
- provide restricted menus for users, and;
- install security measures whenever feasible.

C. Other: Users are expected to have access to the Technology Acceptable Use Policy. District employees are expected to know and abide by the Technology Acceptable Use Policy and to encourage users to become familiar with it.

D. The LISD’s network is intended for legitimate school business and educational purposes only. As a monitored network, no stated or implied guarantee is made regarding the privacy of any communications transmitted or received over this network.

E. Partnerships with other educational institutions, public and private human services agencies, and other entities intending to use the District’s technology resources to access and transmit electronic data and for other related purposes shall be encouraged within the limits of the District’s legal authority. Equitable financial support from such partners, viewed in light of the contributions made by constituent Districts, shall be considered in the development of any such partnership. The Board of Education reserves the right to approve agreements and contracts establishing technology partnerships regardless of the amount of funds involved. The President of the Board of Education shall be a signatory to such agreements and contracts.

Such agreements or contracts shall include the following prohibitions on the use of access to the LISD's network: uses that infringe upon or compromise the legitimate educational use of electronic information technologies; uses prohibited by law; use for the purchase, sale, and/or advertisement of goods, negotiable paper, or services; and uses that jeopardize resource availability for students and employees. Violations of these prohibitions shall be grounds for termination of the agreements or contracts at the discretion of the Board of Education.

F. The LISD makes no warranties of any kind, whether expressed or implied, for the use of its educational technology, including but not limited to the loss of data resulting from delays, non-delivery, or any service interruption.

G. The LISD is not responsible for any damages caused to a user's hardware or software incurred from connecting to the district's network.

COMPUTER AND COMPUTER NETWORK SAFETY AND USE POLICY
1. In compliance with the federal Children's Internet Protection Act (47 USC 254 (h) and (l)), not later than June 30, 2002 there shall be instituted for the School District's computers and computer network a technology protection measure that protects against Internet (which, as used in this policy, includes the World Wide Web) access by both adults and minors to material which is: obscene; child pornography, or; harmful to minors.

A. The term "minors" means individuals under the age of eighteen (18) years.

B. The term "child pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: 1) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; 2) such visual depiction is, or appears to be, of a minor engaging in sexually explicit conduct; 3) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or 4) such visual depiction is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.

C. The term "materials harmful to minors" means any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that: 1) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; 2) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and 3) taken as a whole, lacks serious literary, artistic, political or scientific value to minors.

2. The activities of students on School District computers and computer network shall be monitored by the teacher responsible for the class for which the computer activity is

being conducted, and/or by School District personnel designated by the Superintendent of Schools.

3. No person shall use any school District computer, computer equipment, or school District-provided Internet connection to access sexually explicit or obscene material.

4. When using school District computers, computer equipment or Internet connections for electronic mail, chat rooms, bulletin boards or any other form of direct electronic communication, no student shall disclose any personal information (including, but not limited to, names, addresses, telephone numbers and photographs) about other students or school District staff. Students shall be discouraged from disclosing personal information about themselves in electronic mail, chat rooms, bulletin boards or any other form of direct electronic communication through the Internet.

5. School District computers, computer equipment and Internet connections shall not be used by any person to access another person's accounts, files, data or information without authorization, or for any unlawful activity. The interference with others' accounts, files, data, or information is prohibited.

6. The school District reserves the right to monitor and review all use of its computers, computer equipment, and computer network (including, but not limited to, Internet activity and external/internal electronic mail, files and data); no user of the School District's computers, computer equipment or computer network shall have any expectation of privacy with respect to use of the School District's computers, computer equipment or computer network.

7. No person shall engage in any activity which is detrimental to the stability or security of the school District's computers, computer equipment or computer network, or use school District computers, computer equipment, or computer network in any way which is detrimental to the stability or security of others' computers, computer equipment or computer networks, including, but not limited to, the intentional or negligent introduction of viruses, or the vandalism or abuse of hardware or software.

8. No person shall use the school District's computers, computer equipment or computer network in violation of copyright laws, including, but not limited to, the installing, downloading, copying or using of copyrighted software without proper authority.

9. No person shall, in the course of using the school District's computers, computer equipment or computer network, impersonate another person or user; no person shall reveal a password of another person or user.

10. No person shall use the school District's computers, computer equipment or computer network for commercial purposes.

11. Violation of this policy may result in disciplinary action, as well as restriction, suspension or termination of access to the school District's computers, computer equipment and/or computer network. In addition, referral may be made to law enforcement authorities.

12. This policy shall not be instituted prior to the giving of reasonable public notice and the holding of at least one (1) public hearing or meeting to address the contents of this policy.