

Lake Arthur Municipal Schools

Instruction

Policy 476: Computer, E-mail, Internet, and Information Technology Acceptable Use Regulations, Procedures, and Forms

ACCEPTABLE USE REGULATION ADDENDUM: COMPUTER, E-MAIL, INTERNET AND INFORMATION TECHNOLOGY ACCEPTABLE USE

“User” shall mean all persons who are granted access to the Lake Arthur Municipal Schools’ computer resources.

“Computer Resources” shall mean all computer hardware, software, communications devices, facilities, equipment, networks, Internet use, passwords, licensing and attendant policies, manuals and guides.

No expectation of privacy. The computers and computer accounts given to Users are to assist them in enhancing student academic achievement and job performance. Users do not have an expectation of privacy in anything they create, store, send, or receive on the computer system. The computer system belongs to LAMS and may be used only for education program purposes.

Waiver of privacy rights. Users expressly waive any right of privacy in anything they create, store, send, or receive on the computer or through the Internet or any other computer network. Users consent to allowing LAMS personnel access to review all materials users create, store, send, or receive on the computer or through the Internet or any other computer network. Users understand that LAMS may use human or automated means to monitor use of its computer resources.

Access to or Creation of inappropriate or unlawful materials. Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, threatening or potentially violent, defamatory, racially offensively proselytizing inappropriate or otherwise unlawful, or in violation of School Board policy may not be created, accessed or sent by e-mail or other form of electronic communication (such as bulletin board systems, newsgroups, chat groups) or displayed on or stored in computers. Users encountering or receiving this kind of material should immediately report the incident to their supervisors.

Prohibited uses. Without prior written permission from the District’s Superintendent or designee, computer resources may not be used for dissemination or storage of commercial or personal advertisements, promotions, destructive programs (including but not limited to self-replicating codes or viruses), political or religious material, or any use which is unauthorized or in violation of School Board policy.

Waste of computer resources. Users may not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending or forwarding mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, sending or forwarding jokes, engaging in online chat groups, printing multiple copies of documents, or otherwise creating unnecessary network traffic.

Misuse of Software. Without prior written authorization from the LAMS Technology Services Supervisor, Users may not do any of the following: (1) copy software for use on their home computers; (2) provide copies of software to any third person; (3) install software on any School District workstations or servers; (4) download any software or run executable files from the Internet, email, or other online service to any LAMS workstations or servers; (5) modify, revise, transform, recast, or adapt any software; or (6) reverse-engineer, disassemble, or de-compile any software. Users who become aware of any misuse of software or violation of copyright law must immediately report the incident to their site administrator.

Lake Arthur Municipal Schools

Instruction

Policy 476: Computer, E-mail, Internet, and Information Technology Acceptable Use Regulations, Procedures, and Forms

ACCEPTABLE USE REGULATION ADDENDUM: COMPUTER, E-MAIL, INTERNET AND INFORMATION TECHNOLOGY ACCEPTABLE USE

Communication trade secrets. Unless expressly authorized by the LAMS Superintendent or designee, sending, transmitting, or otherwise disseminating proprietary data, trade secrets, or other confidential information of LAMS is strictly prohibited.

Responsibility for passwords. Users are responsible for safeguarding their passwords for access to the computer system. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. No User may access the computer system with another User's password or account.

Passwords do not imply privacy. Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on the computer system. LAMS has global passwords that permit it access to all material stored on its computer system, regardless of whether or not material has been encoded with a particular User's password.

Accessing other user's files. Users may not alter or copy a file belonging to another User without first obtaining permission from the owner of the file. A Users ability to read, alter, or copy a file belonging to another User does not imply permission to read, alter, or copy that file. Users may not use the computer system to "snoop" or pry into the affairs of other users or LAMS operational systems by unnecessarily reviewing their files and e-mail without authority.

Assessing other computers and networks. A User's ability to connect to other computers systems through the network or by a modem does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems.

Computer security. Each User is responsible for ensuring that use of outside computers and networks, such as the Internet does not compromise the security of LAMS Computer Resources. This duty includes taking reasonable precautions to prevent intruders from accessing the LAMS network via Internet connections or by leaving systems on and logged into the network without authorization and to prevent the introduction and spread of viruses.

CIPA. All users of the Internet must comply with the Children's Internet Protection Act (CIPA), 47 U.S. C 254. **Internet Safety Policy** Access by minors to inappropriate matter on the Internet and World Wide Web is prohibited on the LAMS network. Using electronic mail, chat rooms, and other forms of direct electronic communications is prohibited on the BCS network. Unauthorized access including "hacking" and other unlawful activities by minors online is prohibited on the BCS network. Unauthorized disclosure, use, and dissemination of personal information regarding minors is prohibited by LAMS. Measures designed to restrict minors' access to materials harmful to minors are in place at LAMS.

Lake Arthur Municipal Schools

Instruction

Policy 476: Computer, E-mail, Internet, and Information Technology Acceptable Use Regulations, Procedures, and Forms

ACCEPTABLE USE REGULATION ADDENDUM: COMPUTER, E-MAIL, INTERNET AND INFORMATION TECHNOLOGY ACCEPTABLE USE

Virus detection. Viruses can cause substantial damage to computer systems. Each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into the LAMS network. To that end, all material received on floppy disk or other magnetic or optical medium and all material downloaded from the Internet or from computers or networks that do not belong to LAMS **MUST** be scanned for viruses and other destructive programs before being placed onto the computer system or network. Users should understand that their home computers and laptops may contain viruses. All disks transferred from these computers to the LAMS network **MUST** be scanned for viruses.

Use of encryption software. Users may not install or use encryption software on any of the LAMS computers without first obtaining written permission from the District Technology Services Supervisor. Users may not use passwords or encryption passwords that have not been provided by the District Technology Services Supervisor.

Export restrictions. The federal government has imposed restrictions on export of programs or files containing encryption technology (such as e-mail programs that permit encryption of messages and electronic commerce software that encodes transactions). Software containing encryption technology is not to be placed on the Internet or transmitted in anyway outside the United States without the prior written authorization from the District Technology Services Supervisor.

Compliance with applicable laws and licenses. In their use of computer resources, Users must comply with all software licenses, copyrights, all other state, federal, and international laws governing intellectual property and online activities.

Other policies applicable. In their use of Computer Resources, Users must observe and comply with all other policies and guidelines of LAMS.

No Additional rights. This Policy is not intended to, and does not grant, Users any contractual rights.

Violation of Policy. Violation of this policy will result in loss of access to network resources, and possible legal and disciplinary action.

FN: InstrReg/StuInfoTechRegExplAddendumPolicy476Reg.doc