

**I. Definitions**

- A. "User" means all persons who are granted access to the Lordsburg Municipal School District's computer resources.
- B. "Computer Resources" means all computer hardware, computer software, communications devices, facilities, equipment, networks, passwords, licensing and attendant policies, manuals and guides.

**II. No Expectation of Privacy**

- A. *No expectation of privacy.* The computers and computer accounts given to Users are to assist them in performance of their jobs. 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 the District for business and/or education program purposes.
- B. *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 personnel of the District to access and review all materials Users create, store, send, or receive on the computer or through the Internet or any other computer network. Users understand that the District may use human or automated means to monitor use of its computer resources.

**III. Prohibited Activities**

- A. *Inappropriate or unlawful material.* Material that is fraudulent, harassing, embarrassing, lewd, sexually explicit, profane, obscene, intimidating, threatening or potentially violent, defamatory, racially offensive, proselytizing, inappropriate, or otherwise unlawful, or in violation of District policy may not be 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.
- B. *Prohibited uses.* Without prior written permission from the District's Technology Coordinator, 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, receipt or distribution of inappropriate or unlawful material as defined above, participation in or accessing chat lines, chat groups or chat sites (unless directly related to the school curriculum and such access has been authorized in advance by the building supervisor, Technology Director, or Superintendent), accessing any site which displays or distributes inappropriate or unlawful material as defined above, or any use which is unauthorized or in violation of District policy.
- C. *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.
- D. *Misuse of software.* Without prior written authorization from the District's Technology Coordinator, 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 District workstations or servers; (4) download any software or run executable files from the Internet, email or other online service to any District workstations or servers; (5)

modify, revise, transform, recast, or adapt any software; or (6) reverse-engineer, disassemble, or decompile any software. Users who become aware of any misuse of software or violation of copyright law must immediately report the incident to their supervisors.

- E. *Communication trade secrets.* Unless expressly authorized by the District's Technology Coordinator, sending, transmitting, or otherwise disseminating proprietary data, trade secrets, or other confidential information of the District is strictly prohibited. Unauthorized dissemination of this information may result in substantial civil liability as well as severe criminal penalties under the Economic Espionage Act of 1996.

#### IV. Passwords

- A. *Responsibility for passwords.* Users are responsible for safe-guarding 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.
- B. *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. The District has global passwords that permit it access to all material stored on its computer system – regardless of whether that material has been encoded with a particular User's password.

#### V. Security

- A. *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. 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 District operational systems by unnecessarily reviewing their files and e-mail without authority.
- B. *Accessing other computers and networks.* A User's ability to connect to other computer 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.
- C. *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 District Computer Resources. This duty includes taking reasonable precautions to prevent intruders from accessing the District's 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.

#### VI. Viruses

- A. *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 District's 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 District 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 District's network MUST be scanned for viruses.

**VII. Encryption Software**

- A. ***Use of encryption software.*** Users may not install or use encryption software on any of the District's computers without first obtaining written permission from their supervisors. Users may not use passwords or encryption passwords that have not been provided to their supervisors.
- B. ***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 any way outside the United States without the prior written authorization of the District's Technology Coordinator.

**VIII. Miscellaneous**

- A. ***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.
- B. ***Other policies applicable.*** In their use of Computer Resources, Users must observe and comply with all other policies and guidelines of the District.
- C. ***Computer configuration.*** The following items are considered user configurable and may be changed by the operator; screen saver, mouse pointers, additions to the Microsoft Office toolbars that do not replace the office standard, and views in mail and other programs. Manipulating computer configuration
- D. items not in this list may be subject to disciplinary action if not authorized by the District's Technology Coordinator.
- E. ***Amendments and revisions.*** This policy may be amended or revised from time to time as the need arises. Users shall comply with all amendments and revisions once adopted by the School Board.
- F. ***No additional rights.*** This Policy is not intended to, and does not grant, Users any contractual rights.

**IX. Violation/Consequences**

- A. ***Students.***
  - 1. Students who violate this policy shall be subject to revocation of district system access up to and including permanent loss of privileges, and discipline up to and including expulsion.
  - 2. Disciplinary action may be appealed by parents and/or students in accordance with existing district procedures for suspension or revocation of student privileges.
- B. ***Staff.*** Staff who violate this policy shall be subject to discipline, up to and including suspension, termination or discharge, in accordance with Board policy, negotiated agreements and applicable law.
- C. ***Violations of law:*** Violations of law by students or staff will be reported to law enforcement officials.