Internet, Intranet, E-mail and Digital Network Usage: Acceptable Use Regulation for Staff and Students

I. Definitions

As used herein:

A. "Access" means the ability to read, change or enter data using a computer or an information system.

B. "District" means Los Alamos Public Schools.

C. "Information technology resources (IT resources)" means all computer hardware, software, databases, electronic messaging systems, communication equipment, computer networks, telecommunications circuits, and any information that is used by the district to support programs or operations that is generated by, transmitted within, or stored on any electronic media.

D. "Mobile data storage media;" includes all forms of computer data storage and transport, including, but not limited to, computer floppy disks, writable CDs and DVDs, solid state storage cards, mobile computer storage and playback devices: including, but not limited to MP3 players, USB and Firewire drives, mobile phones or smart phones and personal digital assistants (PDAs).

E. "Restricted personal data" means data containing confidential personal information including addresses, medical information, financial data as defined by federal or state statute or school board policy.

F. "Security mechanism" means a firewall, proxy, internet address-screening or filtering program, or other system installed to prevent the disruption or denial of services or the unauthorized use, damage, ,destruction, or modification of data and software.

G. "Teacher" means anyone delivering instruction in the classroom including, but not limited to, certified teachers, educational assistants, substitute teachers, and community or parent volunteers.

H. "User" means all persons who are granted access to the district's information technology resources.

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 and education purposes. 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 educational 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 IT 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, inappropriate or otherwise unlawful, or in violation of school board 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 may not use district IT resources for mass dissemination of religious, political, or proselytizing materials. Users encountering or receiving this kind of material should immediately report the incident to their supervisors or teachers. Restricted personal data and student record data under the purview of the Family Educational Rights and Privacy Act (FERPA) shall not be transferred to non-district personal mobile data storage media or non-district owned laptops or computers.

B. Prohibited uses. Without prior written permission from the Superintendent or Superintendent's designee, district IT 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), 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 site administrator), accessing any site which displays or distributes inappropriate or unlawful material as defined above, or any use which is unauthorized or in violation of school board policy. District IT resources should not be used for storage of databases or for services not related to the district's mission, vision or core values. This restriction does not extend to activities and uses appropriate to the personal work environment.

C. Waste of computer resources. Users may not deliberately perform acts that waste district IT resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending or forwarding mass e-mailings or chain letters, spending excessive amounts of time surfing the Internet, playing games, sending or forwarding jokes, engaging in online chat groups, printing an excessive number of copies of documents, or otherwise creating excessive and 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 district licensed software for use on their home computers; (2) provide copies of district licensed software to any third person; (3) install unauthorized software on any district workstation or server; (4) download any licensed software or run executable files from the Internet, e-mail or other online service to any district workstation or server; (5) modify, revise, transform, recast, or adapt any licensed software; or (6) reverse-engineer, disassemble, or decompile any licensed software. Users who become aware of any misuse of software or violation of copyright law must immediately report the incident to their supervisors or teachers.

E. Communication trade secrets. Unless expressly authorized by the Superintendent or Superintendent's designee, 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 district IT resources. Passwords should be changed periodically. Individual passwords should not be printed, stored online, or given to others. **Users are responsible for**

all transactions made on district IT resources using their assigned account and password. No user may access district IT resources with another user's password or account.

B. Passwords do not imply privacy . Use of passwords to gain access to district IT resources 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 system access that permit it access to all material stored on district IT resources-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 district IT resources to "snoop" or pry into the affairs of other users or district operational systems by unnecessarily reviewing their files and e-mail without written 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 IT 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. Users are encouraged to maintain up-to-date anti-virus protection and security updates on home computers to reduce the threat of spreading viruses.

VI. Viruses

Virus detection. Viruses can cause substantial damage to district IT resources. Each user is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into district IT resources. To that end, all material received on floppy disk or other magnetic or optical media and all material downloaded from the Internet or from computers or networks that do not belong to the 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 data 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 or teachers. Users may not use passwords or encryption passwords that have not been provided to their supervisors or teachers.

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 from the district's Technology Coordinator.

VIII. Personal Use of the Internet

Personal use. Occasional personal use of district IT resources and Internet access is allowed subject to limitations. Personal use of the Internet is prohibited if:

A. It materially interferes with the use of district IT resources by district staff, students or for district programs.
B. Such use burdens the district with additional costs.
C. Such use interferes with the user's employment duties or other obligations to the district.
D. Such personal use includes any activity that is prohibited in section III of this agreement.

IX. Internet Safety

A. Internet content filtering. In compliance with the Children's Internet Protection Act (CIPA), the district will implement filtering and/or blocking software to restrict access to Internet sites containing child pornography, obscene depictions, or other materials harmful to minors under 18 years of age as determined by the school board. However, no software is foolproof, and there is still a risk an Internet user may be exposed to a site containing such materials. Protections will also include active teacher oversight and age-appropriate guidance to Internet access. A user who inadvertently connects to an inappropriate site must immediately disconnect from the site and notify a teacher or supervisor. If a user sees another user is accessing inappropriate sites, he or she should notify a teacher or supervisor immediately.

B. Monitoring online activities. Monitoring is aimed to protect minors from accessing inappropriate matter. In compliance with CIPA, the district and its representatives will implement a security mechanism to monitor all minors' online activities, including website browsing, e-mail use, chat room participation and other forms of electronic communications. If such a security mechanism leads to discovering that a user has violated or may be violating this regulation, the appropriate disciplinary code or law will be applied. The district reserves the right to monitor other users' (e.g., employees, students 18 years or older) online activities, and to access review, copy, store or delete any electronic communications or files and disclose them to others as it deems necessary.

C. Posting of personal information. Student information shall not be posted online unless it is for instructional purposes, and only if the student's parent or guardian has granted permission (6145.3R). For example, students should not reveal their full names, home addresses, telephone numbers, school addresses, or parents' names on the Internet. Student use of any website that requires the collection of student personal information must comply with the Children's Online Privacy Protection Act (COPPA). Instructional use of such websites, must be approved prior to their use by site administration and follow COPPA guidelines.

D. Internet arranged meetings. Users who are under the age of 18 shall not meet in person anyone they have met on the Internet without their parent's permission.

X. Miscellaneous

A. Compliance with applicable laws and licenses. In their use of district IT 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 district IT resources, users must observe and comply with all other policies and guidelines of the district.

C. Hold harmless. The district does not warrant that the functions of its IT resources or any of the networks accessible through the system will meet any specific requirements, or that the system will be error-free or uninterrupted. Furthermore, the district shall not be liable for any direct or indirect, incidental, or consequential damages (including lost data or information) sustained or incurred in connection with the use, operation, or inability to use the computer resources.

D. 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.

E. No additional rights. This regulation is not intended to, and does not grant, users any contractual rights.

XI. Violation/Consequences

A. Students.

1. Students who violate this regulation or the Information Technology Code of Conduct shall be subject to revocation of district information technology resource 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 regulations for suspension or revocation of student privileges.

B. Staff. Staff who violate this regulation shall be subject to discipline, up to and including suspension, termination or discharge, in accordance with school board policy, negotiated agreements and applicable law. **A single violation of this regulation of a serious nature which threatens the security of district IT resources or is of a criminal nature may result in immediate termination.**

C. Violations of law. Violations of law by students or staff will be reported to law enforcement officials.

Los Alamos Public Schools
Grade K-2
Technology Code of Conduct

A good computer user:

1. Uses the computer with good intentions. Does not use a computer to hurt people or their work.

2. Respects the computer as the school's property. Does not break or hurt the computer. Reports broken equipment or problems with equipment to a teacher.

3. Practices good computer citizenship. Does not look at, send or print bad or mean messages or pictures.

4. Respects the environment. Does not waste paper by printing too much.

5. Respects the rights of others. Does not go into another person's folders, work, or files without permission.

6. Acts responsibly. Immediately tells an adult if his or her computer shows bad things.

7. Accepts responsibility. Always follows teacher's directions. Expects to be disciplined for misuse of the computer system.

Please sign and return to the school.

I agree to be a good computer user.

_____ _____

Student's Name School

_____ _____

Student's Signature Date

I have reviewed this Code of Conduct with my child, and I expect my child to be a good computer user and Los Alamos Public Schools to supervise and protect my child as defined by Los Alamos Public School's *Internet, Intranet, E-mail and Digital Network Usage* (School Board Policy 6144 and 6144.1R)

_____ _____

Parent/Guardian Signature Date

Los Alamos Public Schools
Grade 3-5
Technology Code of Conduct

A good computer user:

1. Uses the computer with good intentions. Does not use a computer to hurt people or their work.

2. Respects the computer as the school's property. Does not damage the computer or computer system. Reports broken equipment or problems with equipment to a teacher.

3. Practices good computer citizenship. Does not look at, send or print inappropriate messages or pictures.

4. Respects the environment. Does not waste paper by printing too much.

5. Respects the rights of others. Does not go into another person's folders, work, or files without permission.

6. Acts responsibly. Immediately tells an adult if his or her computer displays inappropriate material.

7. Will not reveal his or her full name, home address, telephone number, school address, or parents'/Guardians' names on the Internet.

8. Will not meet in person in a secluded place or a private setting with anyone that he or she has met on the Internet.

9. Respects the law. Does NOT violate copyright laws.

10. Accepts responsibility for proper computer use. Always follows teacher's directions. Knows misuse of the computer system can result in loss of computer privilege or other disciplinary action.

Please sign and return to the school.

I agree to be a good computer user.

_____ _____

Student's Name School

_____ _____

Student's Signature Date

I have reviewed this Code of Conduct with my child, and I expect my child to be a good computer user and Los Alamos Public Schools to supervise and protect my child as defined by Los Alamos Public School's *Internet, Intranet, E-mail and Digital Network Usage* (School Board Policy 6144 and 6144.1R).

_____ _____

Parent/Guardian Signature Date

Los Alamos Public Schools
Grades 6-12
Information Technology Code of Conduct

Use of the district's Information Technology resources, including, but not limited to, all computer hardware, software, databases, electronic messaging systems, communication equipment, computer networks, telecommunications circuits, and any information that is used by the district to support programs or operations that is generated by, transmitted within, or stored on any electronic media., by students of Los Alamos Public School District shall be in support of education and research that is aligned with the district's vision, mission and core values.

Use will be in accordance with regulation 6144.1R and this Code of Conduct:

1. Keep confidential and protect all computer and Internet passwords, access codes or logon information from disclosure to others.

2. Respect the privacy of other users. Do not use other users' passwords. Unauthorized use of passwords, access codes or other confidential account information may subject the user(s) to discipline, and to both civil and criminal liability.

3. Be ethical and courteous. Do not send hate, harassing or obscene mail, discriminatory remarks, or demonstrate other antisocial behaviors. State law prohibits the use of electronic communication facilities to send fraudulent, harassing, obscene, indecent, profane, intimidating or other unlawful messages. See NMSA 1978, § 30-45-1 et seq.

4. Maintain the integrity of files and data. Do not modify or copy files/data of other users without their consent.

5. Treat information created by others as the private property of the creator. Respect copyrights. Software protected by copyright shall not be copied except as licensed and stipulated by the copyright owner.

6. Use the network in a way that does not disrupt its use by others. Do not use the Internet for commercial purposes. Transmission of commercial or personal advertisements, solicitations, promotions, destructive programs or other unauthorized use unrelated to the district's vision, mission or core values is prohibited.

7. Do not destroy, modify or abuse the hardware or software in any way. Users shall report any suspected abuse, damage to equipment or tampering with files to the school district system operators.

8. Do not develop or pass on programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system, such as viruses, worms, "chain" messages, global mailings, ResEdit, etc. Do not "hack" the system. Attempts to gain unauthorized access to confidential information or private directories maintained by the District or to circumvent privacy protections on internal files or non-public restricted files, accounts or directories of any external source is a violation of this Code of Conduct, and may subject the user to civil or criminal liability.

9. Do not use the Internet to view, access, download or process pornographic, obscene, indecent, profane or otherwise inappropriate material.

10. Use of the system to access games and use of computer time for game-playing shall be restricted solely to instances directed and monitored by teachers and to games that address educational goals.

11. Do not reveal one's full name, home address, telephone number, school address, or parents'/guardians' names on the Internet.

12. Do not meet in person in a secluded place or a private setting with anyone one has met on the Internet. Users who are under the age of 18 shall not meet in person with anyone they have met on the Internet without their parent's/guardian's permission.

In addition to disciplinary sanctions which the district may impose upon students under applicable policies, codes of conduct or administrative regulations, the district reserves the right to remove a user's account and deny use and access of the information technology system if it is determined that the user is engaged in unauthorized activity or is violating this Code of Conduct.

Violations of law by students will be reported to law enforcement officials.

Los Alamos Public Schools
Grades 6-12
Information Technology Use Agreement

Each student and his or her parent/guardian must sign this agreement before the student is granted use of the district's IT resources. Please read the *Grade 6-12 Information Technology Code of Conduct* and the *Internet, Intranet, E-mail and Digital Network Usage* prior to signing this agreement. If you have any questions about these documents, contact your son's or daughter's principal or the district's Technology Coordinator.

I understand and agree to abide by the district's acceptable use regulation and the Information Technology Code of Conduct. I understand that the district may access and monitor my use of the computer system, including my use of the Internet, e-mail and downloaded material, without prior notice to me. I further understand that should I violate the acceptable use regulation and/or Code of Conduct, my IT resource privileges may be revoked and disciplinary action and/or legal action may be taken against me.

Student Signature _____ Date_____

Student Name (Print) _____Graduation Year _____

I have read the district's *Internet, Intranet, E-mail and Digital Network Usage* and the Information Technology Code of Conduct. I understand that access to district IT resources is intended for educational purposes and that Los Alamos Public Schools has established safeguards, regulations, and policies to protect my child from exposure to inappropriate material. I also recognize, however, that it is impossible for the district to prevent access to all inappropriate material, and I will not hold the district responsible for information acquired on the computer system when the district exercises age appropriate protections. I have discussed the terms of the *Internet, Intranet, E-mail and Digital Network Usage* (School Board policy 6144 and 6144.1R) and Information Technology Code of Conduct with my child.

I grant permission for my son or daughter to use the computer system and for the district to issue an account to him or her.

Parent/Guardian Signature _____

Parent/Guardian Name (Print) _____

Date _____

Los Alamos Public Schools Employee
Information Technology Use Agreement

Each employee must sign this agreement as a condition for using the district's information technology resources. Please, read this agreement and the *Internet, Intranet, E-mail and Digital Network Usage* carefully before signing. If you have any questions about these documents, please contact your supervisor.

I have read this agreement and School Board Policy 6144 and Regulation 6144.1R. I understand and agree to abide by the *Internet, Intranet, E-mail and Digital Network Usage.*

I understand that the district may access and monitor my use of district IT resources, including my use of the Internet, e-mail and downloaded material, without prior notice to me. I further understand that should I violate the acceptable use regulation, my district IT resource privileges may be revoked and disciplinary action and/or legal action may be taken against me.

Employee Signature _____

Employee Name (Print) _____

Location _____

Date_____