MARYSVILLE JOINT UNIFIED SCHOOL DISTRICT

Employee Technology Acceptable Use Policy and General Guidelines

[Employee Signature required on Page 10]

Board Policy 4040 (Personnel)
Technology Acceptable Use Policy And General Guidelines

The Board of Education provides employees, for educational and business purposes, access to district Information Technology Resources ("ITR"). ITR includes, by way of illustration and not limitation, district computers, the Internet, Intranet, e-mail, telephones, the district internal network and any and all files, and documents and/or records stored therein. The use of this technology is intended for these and no other purposes.

The district will establish policies that regulate the use of this technology and the information developed, transmitted, and downloaded through its use. Administrative regulations will therefore be developed for employee use of district technology and the Internet.

Employees will be required to sign statements agreeing to district regulations prior to having access to district ITR.

Legal Reference:
EDUCATION CODE
51870-51874 Education technology
52270-52272 Education technology and professional development grants
52295.10-52295.55 Implementation of Enhancing Education Through Technology grant program
GOVERNMENT CODE
3543.1 Rights of employee organizations
PENAL CODE
502 Computer crimes, remedies
632 Eavesdropping on or recording confidential communications
VEHICLE CODE
23123 Wireless telephones in vehicles
23123.5 Mobile communication devices; text messaging while driving
23125 Wireless telephones in school buses
UNITED STATES CODE, TITLE 20
6751-6777 Enhancing Education Through Technology Act, Title II, Part D, especially:
6777 Internet safety
UNITED STATES CODE, TITLE 47
254 Universal service discounts (E-rate)
CODE OF FEDERAL REGULATIONS, TITLE 47
54.520 Internet safety policy and technology protection measures, E-rate discounts

Management Resources:
WEB SITES
CSBA: http://www.csba.org
American Library Association: http://www.ala.org
California Department of Education: http://www.cde.ca.gov
Federal Communications Commission: http://www.fcc.gov
U.S. Department of Education: http://www.ed.gov

Adopted: 3/11/08

Background and Purpose

The district has created extensive networks with information, telephone and computing resources for staff and student use. In addition, the district provides a large and continuously growing number of computer workstations, printers, peripherals, software, training and supplies to all sites. These items are provided to allow you and others in the district to perform your tasks effectively in meeting the goals and needs for which the district was established. By nature, design, and function, the district's computer network and resources must provide a relatively "open" environment. While automatic and procedural security controls are in place to prevent or reduce unauthorized access to these resources, the primary responsibility for maintaining the security of this information and its resources lies with you, the employee. Improper use of any of these resources can cause problems related to the needs of some or all employees and students in the district.

Violation of specific local, State, and Federal laws referenced later in this document may call for prosecution under the law including fines and imprisonment. The district may take disciplinary action against employees for misuse of computer, network, and information resources. Employees have no expectation of privacy for any document(s), e-mail(s) or information stored on, sent from, received by, or passing through the district's ITR.

This policy outlines both acceptable and unacceptable use of the district's technology resources. Each employee shall acknowledge receiving these guidelines by signing the Employee Use Agreement (Exhibit 4040.1).

Definitions

"Information Technology Resources" (hereinafter "ITR") constitutes all district computers and accessories (including, by way of illustration and not limitation, CPU's, printers, monitors, scanners, keyboards, storage devices, and mice), the Internet, Intranet, the district's network, e-mail, and any and all files, documents and/ or records stored therein.

Privacy /Monitoring

Employees of the district shall have NO expectation of privacy concerning the use of district computers, the Internet, Intranet, the district's network, e-mail, and any and all files, documents, and/or records stored therein.

The district reserves the right to monitor employee use of ITR at any time. Personal passwords are not an assurance of confidentiality, and the Internet itself is not secure. Any and all files, documents and/ or records that are prepared, maintained, and/or stored on any district computer or other piece of district property, or are physically located on district property, may be accessible by any other person, including other district employees, at any time, and without prior notice.

Information Technology Resources (ITR)

Ownership

ITR are property of the district. Employee using, modifying, moving, or discarding any of these assets must have prior authorization from the Administrator. Approved district procedures must be followed for moving or discarding any ITR's.

Only district-approved equipment is to have a permanent physical connection to the district network. Users should consult with the Director of Administrative Technology for the proper use of personal portable devices. The district IT Department cannot support unapproved ITR. Installation, upgrade, repair or other forms of support will only be performed on official district owned or licensed computers and ITR.

Information Technology Use

Appropriate Use
District provided computers and ITR are to be used for official district business purposes during work hours. Employees may use the computer system for non-business outside of work hours or during breaks, provided the provisions of all district computers and computer related policies are followed.

Inappropriate Use
Storing any personal non-work related files of any kind on a network drive constitutes an inappropriate use. Personal files may be stored on an employee's local computer, however, the district is not responsible for backup, recovery, or transfer of the files. The district may periodically delete personal files located on network drives.

ITR may not be used in a way that negatively impacts the district and/or other users. For example, employees may not attempt to break into computer systems or their resources to which they have not been granted access. Employees may not attempt to maliciously alter, erase, damage, destroy or make otherwise unusable or inaccessible any data, software, computer or network system.

(See "INAPPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES," below, for specific examples of inappropriate use.)

The computer industry faces a continuing onslaught of malicious viruses, worms, and other damaging programs that attack computer and network resources. The district attempts to maintain anti-virus software in order to minimize the impact of these viruses.

Employees should take precautions to protect their computers from viruses, including, by way of illustration and not limitation, the following:
* Avoid opening email attachments from strangers.
* If an employee receives an attachment from an unknown sender, the employee should contact the sender and verify the purpose of the attachment. The employee should ask the sender if he/she is sure no viruses may have invaded their attachment.
* Do not download any software from the Internet unless directed to and authorized by the Director of Administrative Technology or his/her designee.
* Do not share any downloaded software with others until the district IT department has verified that it does not harbor viruses.

Privacy of District Records - Student, Staff, and Business Information

Confidential Records
Both student and employee records are protected by various State and Federal laws including, by way of illustration and not limitation:
California State Statutes:
* Education Code 67100
* Information Practices Act of 1977 (Civil Code section 1798)
* Public Records Act (Gov. Code 6250)
* Penal Codes 502

Federal Statutes:
* Federal Family Educational Rights and Privacy Act of 1974
* Federal Privacy Act of 1974
* Electronic Communications Privacy Act of 1986

It shall be the responsibility of the employee to ensure that sensitive and confidential material is protected from unauthorized use. Employees must take all reasonable precautions to ensure privacy is maintained under the law while handling information in any form, including but not limited to voice, electronic (disk file, diskette, CD ROM, magnetic tape, email, network storage, etc.), paper, photograph, and microfiche information. Included under this precaution is the disposal of any privacy related materials. Employees shall not seek to use personal or confidential information for your own use or personal gain.

To ensure security of confidential or sensitive files, the following procedures shall be followed:

* Removable storage media containing sensitive or confidential materials must be stored in a secure area when not in use.
* Do not leave computers unattended when logged on to the network.
* Log off or lock the display when leaving the immediate work area.
* Ensure that only authorized personnel are using other computers in your work area.
* If sensitive information is displayed on the screen, be sure that no one else can see it.

Student Information System Account

A separate account will be given to employees who require access to the district's Student Information System (SIS). These accounts must be approved by the site administrator. Employees are responsible for maintaining the security of their personal accounts and may not release it for use by any other individual. Employees must accord their SIS user accounts the same significance as their hand-written signature.

Failure to do so by releasing this information to another individual may be considered false representation and result in disciplinary action. (For more information on how to protect a password, see "PASSWORD/LOGIN/ACCOUNT, below). If the SIS account holder is not available and access to the SIS is necessary (Le. new student enrollment necessary for student to attend class, etc.) the school site should contact the district Technology Department for assistance.

Password/Login/Account

User accounts and passwords control access to the information contained on the computer system. The password is for each employee's personal use only. Employees may be given different levels of access to district systems based on their position and supervisor's authorization.

Each district computer user is responsible for any and all access made with their account. No employee shall take control of another computer or login to any computer using another person's account. Employees can protect their account from misuse by:

* Not writing down password anywhere.
* Not sharing password with anyone, other than the district Technology Department.
* Changing the password immediately if it becomes known to anyone else.
* Changing the password on a periodic basis.
* Choosing a password that cannot be easily guessed by others (e.g., not including personal information.)
* Contacting district Technology Department if there is suspected unauthorized use of an employee's account and/ or password.
* Never leaving a workstation unattended while signed on to an account.

Software/Hardware Procedures

Acquisition

All hardware and software installed on district computers or network must be acquired through the district's Technology Department. To request the purchase of new or upgrade hardware and software, a request must be forwarded to the district Technology Department. The district Technology Department, and in some cases, the employee's supervisor, will valuate requests.

Hardware and software acquisition is restricted to ensure that complete record of all hardware and software installed is documented and that the Technology staff can register, support and apply upgrades accordingly.

Installation

The Technology Department, in accordance with the license agreement, will install all hardware and software on district computers. A copy of the applicable license agreement and the original software media will be kept in a safe storage area maintained by the district Technology Department.

License
The district is licensed to use computer software from a variety of companies. The district does not have the right to reproduce this software for use on more than one computer unless expressly authorized by the copyright owner(s). Unauthorized duplication of software may subject the employee, his or her department, and/or the district to both civil and criminal penalties under the United States Copyright Act.

Only software purchased and installed through the procedures outlined above may be used on district computers. Computer users are not permitted to load personal software on district computers, to copy software from district computers for home use, or to download software from the Internet on to the district computers.

Erasure
No employee shall erase software installed on district computers or computer systems, nor shall an employee erase computer files without permission from the district Technology Department or the file owner. Written permission to erase any other file or files shall be obtained before doing so. No employee shall format or erase computer storage devices without written permission from the district Technology Department.

Maintenance of Records
Any and all files, documents, and/ or records of the district, whether computer generated or otherwise, will be maintained and stored in a format that can be downloaded in a hard paper copy format if necessary.

Employees are responsible for maintaining and/ or storing any and all files, documents, and/or records in this fashion so they are accessible to all district employees and, if so required inspection by the public. No district file, document, and/ or record prepared, maintained, and/ or stored on any district computer that has not been stored in a hard paper copy shall be deleted or permanently erased without prior authorization. Incidental e-mail may, however, be deleted by employees. Personal documents, including e-mail, are not to be stored on district computer systems.

Any malicious attempt to harm or destroy data (including the uploading, downloading, or creating of computer viruses) and/or any malicious attempt to harm or destroy district office equipment, materials, files, documents, and/or records is a violation of district policy and may also violate other state and federal laws. Such action may result in disciplinary action against the individual(s) up to and including termination. Such action may result in civil and/ or criminal prosecution.

Internet Use

Appropriate Use
Internet access and use is to be used for official district business purposes during work hours to distribute information or to research district related matters. However, employees may use the Internet for non-district related matters outside of work hours or during approved breaks, provided that no provisions of this and related computer policies are violated.

Inappropriate Use
Common sense and good judgment must be used in determining whether using the Internet for specific purposes will violate this policy. (See "INAPPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES," below, for specific examples of inappropriate use.)

Internet Filtering/CIPA Compliance
The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress in December 2000 to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding support for Internet access or internal connections from the "E-rate" program a program that makes certain technology more affordable for eligible schools and libraries. In early 2001, the Federal Communications Commission (FCC) issued rules implementing CIPA.

To insure CIPA compliance the district utilizes an extensive Internet filter that effectively blocks Web sites that fall under the following categories:

* Alcohol
* Chat
* Child Porn
* Criminal skills
* Cults
* Drugs
* Education Cheating
* Explicit Art
* Free Hosts
* Gambling
* Games
* General pornography
* Hacking
* Hate Groups
* Instant Messaging
* Internal Traffic
* Internet Radio
* Internet Service Provider
* Malicious Code/Spyware/Virus
* Message Boards
* Militant/Extremist/Terrorist
* Obscene/Tasteless
* Peer-to-peer /File Sharing
* Personals
* Public Proxies
* R Rated
* Tobacco
* Unsavory /Dubious
* Weapons
* Web Based Email
* Web Based Newsgroups
* Web Based Storage

For further information on any of these categories, please contact the Director of Administrative Technology. While it is true that most Web sites that fall under these categories are inappropriate for educational purposes, there are times when a Web site that falls under one of these categories should not be filtered. If an employee feels that this is the case, they should request from the Director of Administrative Technology that the Web site be removed from the filtered list. If the Director of Administrative Technology feels that there are reasons that the site should remain blocked, the Director might request that the employee fill out a Web Site Approval Form (Exhibit 4040.2), which will be submitted to the Board of Education for approval.

Use of the E-Mail System

Appropriate Use

The district's E-mail system is to be used for official district business and by district employees only. In drafting any E-mail, employees must keep all messages professional and should never send anything by way of E-mail that would not be appropriate for a letter or memo. Employees use the E-mail system with the understanding that employees have no expectation of privacy for any E-mail (even messages marked as "confidential"), and the district retains the right to monitor the content of any and all messages.

Private or personal non-commercial use of the district's e-mail is permitted as long as it is not excessive and does not interfere with the district's normal business practices and the performance of individual tasks. This use is contingent on an employee's compliance with this policy.

Inappropriate Use
Common sense and good judgment must be used in determining whether an E-mail being sent will violate this policy. (See "INAPPROPRIATE USE OF INFORMATION TECHNOLOGY RESOURCES," below, for specific examples of inappropriate use.)

Employees must report to the district Technology Department, any Emails received from outside sources that contain discriminatory, offensive, defamatory or harassing content. Employees that receive unwelcome, offensive material from another employee should report the incident to their supervisor immediately. Supervisors, administrators and the IT district staff that investigate reports of unsolicited material must take reasonable steps to protect the confidentiality of the individuals involved.

E-mail Retention and Destruction
The district maintains an ongoing backup schedule of computer data in order to ensure that these facilities may be restored to use in the event of damage and/ or destruction. Because of this practice, email may be stored on backup media for extended lengths of time. Messages which a user assumes to be deleted may be able to be restored if demanded by the appropriate district authority. Each user should consider whether he/she wants to archive his/her personal messages to their workstation's hard drive or other disk media on some sort of regular basis, as there is always the possibility that information may be lost due to software or hardware problems.

Users should be careful not to consider email as a long-term filing system. While the district maintains a backup of all email, it is not feasible nor our practice to restore lost or damaged email.

Classroom Use of E-mail by Students
The district may contract with an external service to provide email accounts for students. These accounts can be monitored, and permissions set, by teachers or designated site administrators. Teachers who require students to use email shall direct them to utilize only district-sponsored accounts.

Other Technology

Use of Telephones, Cell Phones, and Voice mail
Telephones and cell phones are provided to conduct the business of the district. In many cases, voice mail is also provided. These services are intended to provide a means of communication for employees to contact parents and students, agencies, vendors, other institutions and government officials.

When using these services, your comportment should be businesslike and professional. Employees must reimburse the district for any charges incurred at the district per minute charge for personal use, regardless of the time of call. Private use of the phones should be kept to a minimum.

Use of District Laptop Computers
Laptop computers may be issued to staff members. They are provided to assist the employee with accomplishing their daily work responsibilities.

These machines are not to be used by students or any other individual other than the person to whom it was issued. Employees are expected to take all reasonable precautions to keep laptops issued to them safe and secure. When transporting laptops off district property, employees should take care to not leave them in unattended automobiles, hot or damp places, or where there is an increased risk of damage or theft.

Employees are to follow established Site checkout procedures for taking laptops home overnight, on weekends, and over holidays and breaks. Employees who choose to take their laptop home must have homeowner's/renter's insurance covering damage or loss of the equipment. District insurance is in force while the machine is on district property. Employees shall provide proof of such insurance to the district Technology Department.

The Employee assumes responsibility for any viruses, inappropriate material and/or any other information or software which was downloaded or otherwise added to the laptop during the period in which it was checked out.

Misuse, abuse, neglect, willful damage, termination of employment, or violation of district policy while using a laptop shall require immediate return of the laptop to the district.

Other Services

Please note that this policy addresses issues common to all teachers and employees. Other specific policies may apply to those working in specialized environments or completing specialized tasks such as advising students involved in web publishing. If you have any questions about this or other policies, please do not hesitate to ask the Director of Administrative Technology.

Violations

An employee who violates this policy may be subject to formal disciplinary actions up to and including termination from district employment. In addition, any employee found to have violated this policy may have his/her computer access limited or revoked.

Violation of copyright and/ or other related laws may result in civil liability, monetary damages and/or criminal prosecution.

Inappropriate Use of Information Technology Resources

By way of illustration, and not limitation, the following constitutes inappropriate use of the district's ITR:

* Generating, sending, requesting, receiving, storing, displaying or accessing offensive material including, but not limited to, sexually explicit material, material containing racial slurs, gender offensive comments or images, or any material that would be offensive on the basis of age, sexual orientation, religious beliefs, national origin, or disability.
* Conducting business for personal financial gain from the use of district resources (e.g. placing or advertising personal items for sale, using a district computer to engage in outside business endeavors, or sending unsolicited E-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (spam.))
* Visiting inappropriate sites allowing the district's domain to be captured, which is likely to result in negative publicity or adverse public reaction. Conducting illegal activities (i.e. gambling, placing wagers or bets, buying drugs).
* Copyright infringement - downloading or forwarding of protected information, or violating licensing laws.
* Logging on to the Internet and leaving it running all day when not related to district business.
* Downloading non-approved hardware or software (including personally owned hardware or software) to district computers without prior authorization from the Director of Administrative Technology or his/her designee.
* Creating acts of fraud, waste or abuse through Internet activities.
* Using any type of Instant Messaging software (e.g., AOL Instant Messenger, MSN Messenger, ICQ).
* Downloading items in excess of 20 kilobytes.
* Any activity that could result in negative publicity or adverse public reaction.
* Unauthorized use of another user's computer account or a system computer account.
* Employees should exercise caution in transmitting sensitive or confidential information or documents via the E-mail system or the Internet. Such documents or information include, by way of illustration and not limitation:
* Employee personal information and files;
* Student records.
* Generating, sending, receiving or requesting items of political nature or having to do with political activities.
* Creating and sending messages from another employee without his or her permission.

* Using the district E-mail system for an E-mail subscription service that is not related to district business, including way of illustration and not limitation, newsletters or distribution lists.
* Downloading any non-district business material to any district system (i.e. printers, hard-drives, etc.).
* Sending, receiving or forwarding jokes, 'cute' attachments, or chain letters.
* Opening, sharing or res ending any file attachments received via E-mail, unless there is a specific business reason to do so. This includes, by way of illustration and not limitation, executables, graphics, documents, and spreadsheets.
* Using your district E-mail address to fill out an Internet-based form.
* Any form of harassment via E-mail, telephone or paging, whether through language, frequency, or size of messages.
* Unauthorized use, or forging, of E-mail header information.
* Downloading and using internet music programs.

Dated: 3/11/08

Exhibit 4040.1 (Personnel)
Technology Acceptable Use Policy And General Guidelines
Employee Use Agreement

1. Employees shall be responsible for the appropriate use of technology and shall use the district's information technology resources (ITR) only for purposes related to their employment during contractual hours. Such use is a privilege, which may be revoked at any time. Private or personal non-commercial use of ITR is permitted as long as it is not excessive and does not interfere with the district's normal business practices and the performance of individual tasks.

2. Employees of the district should be aware that they have no expectation of privacy concerning the use of district computers, the Internet, Intranet, the district's network e-mail, and any and all files, documents, and/or records stored therein. District ITR should not be used to transmit confidential information about students, employees, or district affairs.

3. To ensure proper use, the Superintendent or designee may monitor the district's ITR, including e-mail and voice mail systems, at any time without advance notice or consent. If passwords are used, they must be available to the Superintendent or designee so that he/she may have access when the employee is absent.

As an employee of the Marysville Joint Unified School district, I have read the above information about the appropriate use of computers in the Marysville Joint Unified School district. I have also received a copy of Board Policy and Administrative Regulation 4040. I understand that a copy of this agreement will be kept on file at my worksite.

As a user of the school computer network, I agree to comply with Board Policy and Administrative Regulation 4040 and to use the network in a constructive manner.

_____ _____

Print Name *Employee Signature*

_____ _____

Date *Primary Worksite*

Dated: 3/11/08

****

Document dated: 5/24/10