

## **Personnel**

### **Employee Use of Technology**

#### **Computer/Online/Internet Services: User Obligations and Responsibilities**

Employees, including members of the School Board, are authorized to use District equipment to access the Internet or other online services in accordance with Board Policy, the District's Acceptable Use Agreement, and the user obligations and responsibilities specified below.

Employees recognize that electronic mail accounts issued through the District are not private. Email delivery is not guaranteed. Authorized personnel may conduct searches of District electronic information systems, email, employee workspaces, student workspaces, and network equipment at any time and without notice when deemed appropriate, including searches for work-related and investigatory purposes. Personal devices connected to District network or computing resources may also be searched when brought to or used at work.

1. The employee in whose name an online services account is issued is responsible for its proper use at all times. Employees shall keep account information, home addresses, and telephone numbers private. They shall use the system only under the account number to which they have been assigned.
2. Employees shall use the system safely, responsibly, and primarily for work-related purposes.
3. Employees shall not access, post, submit, publish, link or display harmful or inappropriate matter that is threatening, obscene, disruptive, excessively violent, or sexually explicit, or that could be construed as harassment or disparagement of others based on their race, ethnicity, national origin, sex, gender, sexual orientation, age, disability, religion, or political beliefs.

*(cf. 4030 Nondiscrimination in Employment)*

*(cf. 4031 Complaints Concerning Discrimination in Employment)*

*(cf. 4119.11 Sexual Harassment)*

4. Employees shall not use the system to promote unethical practices or any activity prohibited by law, Board policy, or administrative regulations.

*(cf. 4119.25 Political Activities of Employees)*

5. Employees shall not use the system to engage in commercial or other for-profit activities without permission of the Superintendent or designee.

6. School-level and district-level email address lists are for professional communications that directly support the educational purposes of the District. Employees shall not use the district's network to transmit general or "mass" emails of a personal, non-professional nature to other district employees without the prior consent of the Superintendent or designee (for use of district-level email lists) or the Principal or designee (for use of school-level email lists.) Personal, non-professional emails sent to e-mail addresses managed by the District using general or "mass" email lists without such prior permission will be considered an abuse or disruption of the email service.
7. Copyrighted material shall be posted online only in accordance with applicable copyright laws.
8. Employees shall not attempt to interfere with other users' ability to send or receive e-mail, nor shall they attempt to read, delete, copy, modify, or forge other users' e-mail. This includes either the creation or promotion of spam, the distribution of viruses or potential viruses, and/or any attempt to bypass or interfere with the orderly operation of the District's network in any way.
9. Employees shall not develop any classroom or work-related web sites, blogs, wikis, forums, or similar online resources representing the District or using District equipment or resources without written permission of the Superintendent or designee. Employees who develop online resources will regularly monitor them for appropriate content for as long as the resources are available online, including all content created by other users of the resource. Online content created by employees containing photographs, video, or audio recordings of students or student work must meet District posting requirements including acquiring signed parent permission before posting. The District retains the right to delete material on any such online resources. Employees who place such resources on the net shall be familiar with the requirements of the Family Educational Right to Privacy Act (FERPA) and shall take care to respect District policy and any state and Federal laws that pertain to student and individual confidentiality.
10. Employees shall report any security problem or misuse of the services to the Superintendent or designee. This includes any attempts to bypass, interfere with, or subvert any content filtering system implemented or adopted by the District.
11. Employees recognize that District Computer resources are not unlimited. User shall not deliberately perform acts that waste or unfairly monopolize resources to the exclusion of others. These acts include unnecessary use of storage, equipment, downloading or uploading of files, chat, casual access of streaming audio, video, and complex graphics files, and any other creation of unnecessary loads on network traffic not associated with District business.
12. The transmission of information about students or District affairs shall adhere to the following:

- Confidential information should never be sent or forwarded to outside individuals or outside agencies not authorized to receive that information. This includes individuals within the District who are outside your department unless there is a clear work-related purpose for doing so.
- Confidential messages and information should never be sent or forwarded to others, including faculty, staff and students who do not need to know the information.
- Confidential information should not be forwarded to multiple parties unless there is a clear and legitimate need to do so. Employees need to be aware that once an email or document is forwarded the sender loses all control over access to the information and document.
- Confidential email should not be retained in an employee's personal mailbox, but should be deleted as soon as possible. Records that need to be kept should be printed and retained according to appropriate policy or regulation.
- Confidential messages from or to legal counsel should not be forwarded to others without counsel's authorization, since such messages may constitute privileged communications between the District and its attorney.

NOTE: Confidential information includes, but is not limited to, Personal Information such as an individual's first name or first initial and last name, in combination with a Social Security number, driver's license number, California identification card number, account number, credit or debit card number; Medical Information, such as diagnosis, medical history, mental or physical condition or treatment plans; Health Insurance Information, such as the individual's health insurance policy number, or claims history; Personnel File Information; Student Records; or similar materials the disclosure of which would constitute an unwarranted invasion of personal privacy.

#### E-mail Retention and Disposal:

E-mail stored on official District systems will generally be preserved for no longer than one (1) year after they have first appeared on the server. Log files associated with e-mail messages which generally provide a record of actual e-mail transactions, but not the e-mail content, will be kept for three (3) years.

E-mail Users storing messages on District servers often have the capability to "archive" e-mail items to files. This effectively allows users to save any e-mail messages that they choose to save for any length of time. These retention and disposal guidelines do not apply to e-mail archives and backups done by individuals.

E-mail correspondence and associated documents sent as attachments may be considered public records. As such, they may need to be retained longer than the established policy guidelines for e-mail retention and disposal. It is the responsibility of the sender and recipient of these e-mail messages to determine the required retention period to comply with applicable District student and personnel records policies and procedures regarding record retention and to preserve these e-mail records either electronically or in printed form with all of the associated header and transmission information.

**Acceptable Use Agreement for Employee Use of Technology**

This agreement applies specifically to the requirements of Board Policy 4040 and Administrative Regulations 4040. A signature at the end of this agreement is binding, and indicates that the party who signs it has carefully read and understood the significance of this agreement's terms and conditions. No user has permission to access the Internet or use school District computers without this signed and dated agreement on file with the school and/or District.

I understand and will abide by the above Acceptable Use Agreement. I further understand that any violation of the regulation is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and school/District disciplinary action and/or appropriate legal action may be taken including possible suspension or termination.

\_\_\_\_\_  
Employee Signature:

\_\_\_\_\_  
Date:

Adopted: June 24, 2009  
Revised: August 25, 2010, April 11, 2012

**WEST SONOMA COUNTY UHSD**  
Sebastopol, California