

Technology Acceptable Use Policy and Agreement (AUPA) Westminster School District Employees

General Provisions

1. Purpose

The purpose of this policy is to allow Westminster School District employees access to technology resources while protecting the District against unauthorized access and abuse. WSD recognizes that the use of technology is important to the District and its employees. The Technology Acceptable Use Policy and Agreement (AUPA) provides a blueprint for employees to use technology in compliance with the WSD Technology Use Policy (BP 4040).

2. Applicability

This policy applies to the use of all WSD owned or leased technology equipment including, but not limited to:

- a. All hardware owned or leased by WSD includes, but is not limited to: computers, scanners, printers, fax machines, telephones, cellular phones, smartphones, digital readers, pagers, digital music devices, USB devices, and wireless communication devices,
- b. All on-line services provided or maintained for or by WSD: e-mail accounts, Internet sites, log-ins, passwords, data, files, Internet access, voice mail, and information transmitted by, received from, entered into, or stored in WSD technology, and
- c. All software and firmware associated with (i) and (ii).

3. Violations

- a. WSD employees will use technology in a professional manner that is consistent with Board Policy and Administrative Regulations (BP 4040 and AR 4040) and adhere to all security and other guidelines established by WSD. WSD employees will also adhere to all applicable local, state, federal, and international laws relating to access and use of computer systems, software, firmware, and on-line services. WSD will cooperate fully with the appropriate authorities to provide information related to actual or suspected activity that is inconsistent with the law.
- b. Violations of this policy may result in:
 - Revocation of user access (temporary or permanent) and/or
 - Discipline, up to and including termination of employment, in accordance with WSD policies and any applicable collective bargaining agreements.

4. Privacy

- a. All employees shall have no expectation of privacy in any:
 - Message, file, data, document, facsimile,
 - E-mails and other electronic communications, and

- Any other form of information accessed, transmitted, received, or stored on any technology owned, leased, used, moderated, and operated by WSD.
- b. All employees are advised that all forms of electronic communication are deemed to be public record (California Government Code section 6252) and must be disclosed to the public upon request unless the records are exempt from disclosure under the California Public Records Act. Documents may also be subject to disclosure by subpoena or other legal process.
 - c. To ensure the confidentiality of WSD's internal e-mail system and other electronically stored information and data, all employees are expected to use all technology in a manner consistent with WSD legitimate business and educational interests.
 - d. Authorized WSD employees tasked with the supervision and monitoring of the use of technology may access any technology during the course of carrying out their responsibilities. This access includes, but is not limited to, messages and files.
 - e. Authorized WSD employees tasked with the supervision and monitoring of the use of technology will safeguard and protect the confidential and business information of the District, and will adhere to all District Board policies, local, state, federal, and international laws that protect the confidentiality of employee and student information, including but not limited to personal data, user names, passwords, electronic communication, and any other electronic information transmitted, received, or stored in District technology.

5. Installation/Modifications

- a. Any modification or installation of WSD hardware or software must be authorized by the District Technology Department.
- b. Employees are not permitted to modify existing hardware.
- c. Employees who connect personal technology equipment to the WSD computer network are subject to the Acceptable Use Policy and Agreement.

6. Acceptable Uses

- a. Education or research consistent with the WSD Board Goals.
- b. Authorized business conducted by and for the District ensuring that the user's personal statements are not attributed to the District.
- c. Productivity, information access, communication, and problem solving to support the goals of the District.
- d. All tools and resources provided by WSD that include, but are not limited to computing equipment, Intranet, and Internet to support the Board Goals and meet board policies.
- e. Employees unsure about whether a particular use is acceptable or appropriate should consult their supervisor or the appropriate District personnel for clarification and authorization.

7. Unacceptable Uses

- a. Use of District technology to conduct activity that includes, but is not limited to:
 - Defamation, copyright infringement, violation of contracts, and transmission of materials that violate state and federal laws,
 - Private financial or commercial gain and/or advertising,
- b. Unauthorized access through e-mail, chat rooms, social networks or other means of electronic communication and/or sharing that includes, but is not limited to:
 - Resources, entities, personal data of individuals, electronic communication,
 - Student data and records, and
 - Using another person's account or password and/or disclosing or sharing passwords, thereby compromising the District computer systems.
- c. Creating, communicating, using, or knowingly accessing images or text that are obscene, pornographic, spamming, inflammatory, harassing, threatening, degrading, or harmful to minors or that promote illegal, discriminatory, or unethical activities.
- d. Deleting, copying, modifying, or forging other users' names, e-mails, files, or data.
- e. Disguising one's identity, impersonating other users, and/or sending anonymous e-mails.
- f. Accessing, transmitting, or downloading files such as "chain letters" and "pyramid schemes."
- g. Interfering with other users' ability to access their accounts.
- h. Downloading games, entertainment software, and other software using District technology for personal use.
- i. Accessing and/or viewing information that promotes gambling, illegal drugs, terrorism, theft, or espionage.
- j. Propagating computer viruses and similar malware.
- k. Streaming audio or video that does not support WSD goals.

8. Copyright and Intellectual Property

- a. Employees may access electronic resources and materials that are protected by copyright, trademark, patent, trade secret, and export laws.
- b. Employees may not assume that any information that is accessible through District technology may be downloaded and /or disseminated.
- c. Employees must ensure that any materials accessible through District technology will not violate applicable laws or intellectual property rights of any third party.

- d. Employees may not copy, post, or distribute any WSD proprietary information or any material protected by copyright, trademark, patent, trade secret, and export laws.

9. Security

- a. Employees agree to comply with the Children's Internet Protection Act (CIPA) at all times when using any technology.
- b. Employees are responsible for their user names and password and must keep these secure. The District will take reasonable precautions to maintain the confidentiality of passwords except when disclosure is required by law. Employees should contact the District Technology Department to obtain a new password if lost or compromised.
- c. Employees agree to report a security problem immediately to a supervisor.
- d. The District shall not be responsible for loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions regardless of cause.
- e. The District reserves the right to delete any electronic material, without notice, from e-mail and web pages violating the WSD Acceptable Use Policy and Agreement.

10. Political and Religious Activities of Employees

Employees may not engage in any non-government related fundraising or public relations activities such as solicitation and or lobbying for religious and political purposes.

E-mail Provisions

1. Guidelines

- a. The use of District technology resources is a privilege, not a right, and misuse may result in the temporary or permanent restriction or cancellation of the employee's account.
- b. All e-mail messages and all electronic correspondence are the property of WSD and subject to Board policies, Administrative regulations, office policies, and District procedures and control.
- c. E-mail communication requires the following:
 - A subject title,
 - Use professional language,
 - Brief, clear, and concise language, and
 - The *WSD E-mail Disclaimer will be added at the bottom of the e-mail.
- d. Announcements to "all employees" require approval from the employee's supervisor. Any announcement, such as birth, death, or marriage notices to "all employees" will be sent only by the WSD Superintendent's representative.

2. Violations

- a. Employees, without proper authorization, may not post a message in any Electronic Information System that may be reasonably interpreted as representing the policy of WSD.

- b. Employees are responsible to manage their own mailbox space and should archive or delete messages to ensure space availability.
- c. Employees assume responsibility for any messages sent using their e-mail account.

3. Acceptable Uses

- a. Communication and document transfer that is necessary to conduct the business of the District including, but not limited to:
 - Interdepartmental business
 - Transactions that do not require a signature
 - Authorized vendors
 - State and federal agencies
 - District approved partnerships and collaboratives
 - Scanned and approved signed documents.

4. Unacceptable Uses

- a. Communication and document transfer that requires a signature but is unsigned.
- b. Any confidential personnel information includes, but is not limited to:
 - Employee benefits,
 - Hiring, transfer, or termination, and
 - Resignation or retirement notification.
- c. Personal information that includes salary, address, phone numbers, social security number, documentation of performance, and/or medical condition of students, parents/families, and staff.
- d. Communication that promotes activity violating WSD Board policy and/or state and federal law.

5. Security

- a. Employees should report any electronic security problem to the Technology Department.
- b. Employees will be removed from the system when they have separated employment or are on Leave of Absence for one year or more. It is the employee's responsibility to remove/delete all personal files.
- c. WSD complies with the applicable provision of the Children's Internet Safety Act (CIPA) and will cooperate with the appropriate authorities as required.
- d.

6. Retention of e-mail records

All electronic files and e-mails that are sent, received, and/or stored using District technology shall be retained in accordance with WSD Board policy on Records Retention.

Internet/Web Sites and Usage

1. Guidelines

- a. WSD ensures that all District computers with Internet access have a technology protection measure that blocks or filters Internet access to visual depictions that are obscene, pornographic, or harmful to minors and enforces such measures.
- b. WSD employees that require broader access than defined in (i) may request such access in writing. This includes Web 2.0 social networking sites including, but limited to Facebook, Twitter, wikis, and chat rooms. The request must include educational criteria that support the request.
- c. Web 2.0 “limited public forum” (a site restricted to certain groups and dedicated to the discussion of certain subjects) may reasonably restrict speech and maintain viewpoint neutrality.
- d. All Web 2.0 sites shall be monitored and any complaints shall be directed to the Assistant Superintendent of Human Resources for investigation.

2. Legal requirements (CIPA Compliance)

WSD complies with the provisions of the Children’s Internet Safety Act (CIPA), 47 U.S.C. 254.

3. Digital Millennium Copyright Act Compliance (DCMA, 1998)

- a. WSD will remove any material that infringes or violates copyright.
- b. WSD shall terminate access to employees that are repeat infringers of copyright.
- c. All notification of infringement shall include:
 - The signature of the copyright owner
 - An identification of the infringed work
 - Contact information of the complainant
 - A statement from the complaining party stating that permission was not granted to use the material in question
 - A statement that the information is accurate, and under penalty of perjury, that the complaining part is authorized to act to protect an exclusive right that has allegedly been infringed

4. Social Networking Sites Acceptable Uses

- a. Employees may create Web 2.0 sites that are approved by the employee’s supervisor and appropriate cabinet member or designee and meet the WSD web Authoring Standards to be used internally by WSD employees only.
- b. Employees may create Web 2.0 sites that include postings from individuals outside WSD and must be approved by the employee’s supervisor and the Assistant Superintendent of Human Resources to determine the nature of the forum and the ability of WSD to exclude certain types of materials from the site without violating the free speech rights of the individual.

5. Social Networking Sites Unacceptable Uses

- a. Employees may not create Web 2.0 sites to be used in WSD that constitute a “designated public forum” (a forum that allows posting on any topic).
- b. Any Web 2.0 or like site that posts any material that violates Board policy, state, and federal law shall be removed immediately. These postings may include but are not limited to material that is:
 - Obscene, pornographic (adult and children)
 - Promoting illegal activity
 - Harmful to minors (47 U.S.C. 254)
 - Disclosing employee or student confidential information
 - Promoting the use of alcohol, tobacco, or illegal drugs
 - Advocating violence, hate groups, or other dangerous groups
 - Threatening
 - Discriminating against people based on a protected characteristic
 - Advertising a product or service
 - Violating copyright law
 - Defamatory
 - Private information and may include, but is not limited to photographs, personal information, addresses, and telephone numbers without that person’s permission
 - Promoting or detracting political or religious issues, candidates, ballots, or propositions
- c. Employees shall not permit students to access WSD computers containing Web 2.0 sites unless the site was created specifically for a class, is monitored by the teacher for content, is accessible by both parents and students, and excludes individuals that are not authorized to access the site or violate the WSD AUPA.

6. WEB Site Hyperlinks

- a. Unless authorized, no person shall use the names of:
 - Westminster School District,
 - Westminster School District Board of Trustees, and
 - Westminster School District Superintendent

To suggest imply, or indicate that any corporation, firm, association, group, activity, or enterprise is connected or affiliated with, or is endorsed, favored, or supported by, or opposed by any of the above.
- b. Use of the above names as well as hyperlinks to outside websites may be approved in writing by a Cabinet member or designee if it is determined that such use is in the Department’s best interest.

7. WEB Authoring/Publishing Standards

- a. Purpose of the Standards for Publishing:
 1. These standards provide direction to WSD employees regarding publishing on the Internet through WSD. Consideration reflected in these standards are:
 - Protecting the welfare of students,
 - Respecting the rights of minors and their parents/guardians and families,
 - Protecting every individual’s right to privacy,

- Protecting intellectual and property rights of ownership and/or copyright, and
 - Assuring that web resources are used to promote WSD's educational goals.
- b. Directions for Publishing Web Sites:
1. All web site development will be under the auspices of the Information Technology Department.
 2. All web sites will follow the approval process for publishing and ensure that these meet the WSD AUPA requirements.
 3. After a web site is published, web site content management will be the responsibility of the department owning the web site, and must be maintained.
 4. Web sites within the WSD web site are authorized only if these are created and maintained to provide educational information, resources, and links of interest to students, parents, community, and WSD staff.
 5. Web pages reflect WSD and must be presented in a professional manner, as these are viewable by anyone with Internet access regardless of who created them.
- c. Directions for Publishing Student Information, Work, and/or Pictures
1. Acceptable publishing:
 - A student's original work with written parent permission to be kept on file as long as the work is observing copyright law.
 - Pictures of students taken as a group at an angle or distance so that any one student cannot be easily identified. Parent permission from all students in the picture must be kept on file.
 2. Unacceptable publishing:
 - A student's full name and/or personal information about the student and his/her family.
 - Student work that includes third party content without copyright permission in writing.
 - Pictures of students or student work without written parent permission.
- d. Directions for Publishing Employee Information and Pictures
1. Employee pictures with written permission from the employee may be published.
 2. An employee's personal information may not be published.
- e. Web Publishing and Copyright Law Guidelines
1. Assume all materials are copyrighted unless otherwise stated.
 2. Do not re-publish any text or graphics found on any WSD web site or on the Internet without written permission (to be kept on file).

3. When re-publishing the work of another person, credit to the original author must be included at the bottom of the web page, include the URL of the re-published work where the original is found, and include information regarding how and when the original author granted permission for publication.
4. When re-publishing public domain documents, a citation that evidences public domain must be included at the bottom of the web page.
5. Use only original graphics or public domain images. Do not use third party images, including student-created images.
6. Properly cite online resources.

8. Authoring Standards and Guidelines

- a. When authoring a web page, the following guidelines must be observed:
 1. All content, written and otherwise, reflect WSD goals in a professional manner.
 2. All content must be proofread carefully and checked for grammar and spelling errors before posting.
 3. Linking personal pages of employees, students, parents/families, or community members is not permitted.
 4. All published content must be current and maintained.
 5. Use humor and satire carefully to avoid misinterpretation.
- b. Responsibility for content
 1. All web pages are the property of WSD and subject to review, editing, and/or removal by the Superintendent or his/her designee.
 2. Department and site supervisors in addition to web authors are responsible for content published on the web site.
 3. All individuals named above will be responsible for ensuring that the web pages reflect the WSD Authoring Standards and Guidelines.
 4. WSD requires all web site authors to complete WSD training on web authoring before publishing a web site.
- c. Author's Responsibilities
 1. Employees are required to adhere to the WSD Authoring Standards and Guidelines when posting content on a web page.
 2. The employee's supervisor is responsible for the implementation of the WSD Authoring Standards and Guidelines and for the removal of unauthorized content from the pages of employees under his/her supervision.

- d. Department/Site/Program Webpage Responsibilities
 1. Each department/site/program shall designate a webpage manager who will be responsible, under the direction of the supervisor, for posting and updating content to keep the information on the web site current and accurate.
 2. The designated webpage manager must ascertain from the supervisor that content is accurate and current and that an administrator and/or supervisor have approved it for posting.

***WSD E-mail Disclaimer:**

This communication and any documents, files, or previous e-mail messages attached to it, constitute an electronic communication within the scope of the Electronic Communication Privacy Act, 18 USCA 2510. This communication may contain non-public, confidential, or legally privileged information intended for the sole use of the designated recipient(s). The unlawful interception, use, copy or disclosure of such information, or attempt to do so, is strictly prohibited under 18 USCA 2511 and any applicable law. If you have received this e-mail communication in error, please immediately notify the sender by return e-mail and delete the original e-mail from your system.