ELECTRONIC INFORMATION SYSTEM

General

The System is limited to educational and work-related use. Access is not authorized for purely personal use. The District reserves the right to authorize, limit and prioritize access to and use of the System.

All use of the System must conform with state and federal law and District approved network provider policies and licenses. Use of another organization's network or computing resources must also comply with the rules appropriate for that network.

The unauthorized installation, use, storage, or distribution of copyrighted software of materials on the System is prohibited.

Staff shall be responsible for overseeing the appropriate use of the System by students and shall immediately report any infractions in accordance with District and school rules and regulations.

From time-to-time, the District may determine that specific uses of the System are not consistent with the guidelines and procedures stated above. The District reserves the right to modify or revise these guidelines and procedures at any time. In addition, the information Technology Services Department may block specific software or services commonly known to be in conflict with these procedures.

Users are responsible for the appropriateness and content of material they access, store, transmit, or publish on the System.

Use of the System for any of the following purposes is strictly prohibited:

- Disrupting the operation of the System in any way;
- Destroying, modifying, or abusing System components, including hardware or software;
- Creating or uploading viruses or other harmful code or to intentionally destroy the data of others;
- Gaining unauthorized access to any computer, server or network;
- Possession, installation or use of software, utilities or tools to gain unauthorized access;
- Soliciting or advertising for commercial purposes;
- Accessing, uploading, downloading, storing, or distributing obscene or pornographic material, or materials that contain sexually explicit or indecent subjects;
- Supporting or opposing political candidates or ballot measures;
- Supporting religious worship, exercise, or instruction, of any religious establishment;
- Transmitting or publishing abusive, libelous, defamatory, or discriminatory statements or images, or for any form of antisocial or illegal behavior;
- Bullying, harassing, or intimidating another user, as defined in the District's anti-bullying policy, via online means.
- Circumventing established Internet filtering to gain access to inappropriate material.

System Administration

The Superintendent shall appoint a Director of Information Technology Services who shall be responsible for implementation and oversight of the System in accordance with District policy and procedures.

The Superintendent, Director of Information Technology Services or designee may revoke System privileges to prevent unauthorized activity. In addition, violation of any of the conditions of use may be cause for disciplinary action.

The Director of Information Technology Services and building principals may jointly designate building-level System coordinators that may be delegated administrative responsibilities as appropriate. All building-level System guidelines must be submitted to the Director of Information Technology Services for approval.

Computers, servers, peripherals and other components of the System are property of the District. The District does not grant exclusive rights of use and reserves the right to restrict any customization deemed harmful or unnecessary including, but not limited to, screen savers, search toolbars, and saved personal photo/audio/video files. Computer workstations may be restored to a defined District standard at any time.

Only District owned computers and devices may be connected to the System.

Users are responsible for backing up data files, which can include network shared drives, CD-RW's, floppy disks, or other media. The Information Technology Services Department is responsible for regular backups of network servers for disaster recovery purposes; however, individual files are not easily retrieved.

Electronic Mail ("email")

District provided electronic mail may be used for educational and other work-related purposes.

Information transmitted by email is not necessarily secure, private, or confidential. Users should avoid sending anything in email that might cause harm or embarrassment to themselves or others if revealed to persons other than the intended recipient. For example, messages can be forwarded to anyone else on the System, with or without the knowledge of the original sender. Because email is not confidential, it should not be used to transmit information of a private or personal nature.

Email on the District network is considered public record and is subject to the Public Access to District Records policy #4040 and also personnel or criminal investigations. Email can be retrieved and read even after it has been deleted. The District reserves the right to monitor email use and to access and review any email stored on the System or District equipment.

The security provisions of the email system must be honored at all times. For example, users shall not attempt to gain access to the messages of other users without their consent or the approval of the System Administrator or designee. Professional staff are, however, to supervise student use and may review student electronic communication without limitation.

Good judgment must always be employed when using email. Users are expected to abide by rules of email etiquette, including, but not limited to, being polite, not sending abusive or "flaming" messages, and using appropriate language. The use of profanity or clearly offensive language is prohibited.

In addition to the general guidelines above, the following practices are specifically forbidden:

- Intentionally impersonating or misrepresenting the identity of a sender or receiver of email;
- Modifying a message and forwarding it without noting the changes (i.e. additions, deletions, modifications to the content, etc.);
- Bypassing the user-security mechanisms of the email system in a malicious manner (such as creating bogus accounts or unauthorized "snooping" through mail addressed to others); and
- Placing information on the email system that would defame, or portray in a false light, the sender or recipient of an email message.

Internet

Users must regard and respect copyright, trademark, and license notices in all material and information accessed through the Internet. Accessing the Internet to make infringing uses of copyrighted or other proprietary materials is prohibited pursuant to Policy 2025.

Using the System to access Internet resources including, but not limited to, those that contain sexually explicit or indecent materials, or which promote hate, violence, or discrimination on the basis of race, national origin, religion, sex, or disability is strictly prohibited. Any user who knowingly accesses such sites without the approval of the System Administrator shall be subject to disciplinary action in addition to loss of System privileges. Any user who inadvertently accesses such sites must report the access in accordance with building guidelines.

In accordance with the Child Internet Protection Act, the District maintains and support software that is utilized to block groupings of Internet sites, which are inappropriate for student viewing. As the number of Internet sites grows daily around the world, some inappropriate sites are not grouped properly and may become viewable by students from District-owned computers. The purpose of this procedure is to provide teachers and school administrators a clear process by which sites they deem to be inappropriate can be reviewed and blocked by Information Technology Services.

Whenever a school staff member views an Internet site from a computer on the District network that the member deems to be inappropriate for student viewing, the staff member shall contact the Information Technology Services Department to have the site reviewed and blocked, if appropriate.

If a school staff member views a blocked Internet site and deems it to be appropriate for student viewing, the staff member shall contact the Information Technology Services Department to have the site reviewed and unblocked, if appropriate.

If there is a question as to the instructional validity of a site (blocked or unblocked), the Assistant Superintendent of Instructional Services shall review the site and make the final determination.

Staff members may be provided with a temporary bypass to the internet filter to review questionable web sites. This bypass should not be used to repeatedly visit sites that are blocked by the Internet filter.

Access Security

Users will utilize password facilities to ensure that only authorized users can access the System. When a computer is located in an open space or is otherwise difficult to physically secure, consideration should be given to enhanced password protection mechanisms and procedures.

The maintenance of passwords is the individual responsibility of each user. Passwords are the gateway to the protection of sensitive information including data records of clients, students, and

staff. The system administrator reserves the right to reject passwords that are unsecure, such as not having enough characters or being easy to guess.

For maximum password security, the following steps are strongly recommended:

- Passwords should be eight characters or more.
- Avoid words found in the dictionary and include at least one numeric character.
- Choose passwords not easily guessed by someone acquainted with the user. (For example, passwords should not be maiden names, or names of children, spouses or pets.)
- Do not write passwords anywhere, other than a sealed envelope as part of a building password management system.
- Change passwords periodically.
- Do not include passwords in any electronic mail message.
- Never store passwords or any other confidential data or information on a laptop or home PC or associated floppy disks, CD's or USB drives. All such information should be secured after any connection to the District network.

System accounts are to be used only by the authorized owner of the account for the authorized purpose. Users may not share their password with another person or leave an open file or session unattended or unsupervised. Account owners are ultimately responsible for all activity under their account. The District will provide substitute employees with individual accounts to access the System.

Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the System, or attempt to gain unauthorized access to the System.

Communications and files may not be encrypted to avoid security review. Permissions may not be changed to avoid system administrator review.

Any user who becomes aware of a security problem must notify the System Administrator or designee immediately and must refrain from demonstrating the problem to other users.

Personal Security

Personal information, such as student or staff addresses and telephone numbers, should remain confidential when communicating through the System. Student information shall not be released without parental permission.

Students shall not make appointments to meet people in person that they have contacted through the System without parental permission.

Staff and students shall immediately notify an administrator any time they come across information or messages that appear confidential, inappropriate, threatening, or that otherwise make them feel uncomfortable.

Viruses

Computer viruses are self-propagating programs that infect other programs. Viruses and worms may destroy programs and data, as well as using the computer's memory and processing power. Viruses, worms, and Trojan horses are of particular concern in networked and shared resource environments because the possible damage they can cause is greatly increased. Some of these cause damage by exploiting holes in system software. Fixes to infected software should be made as soon as a problem is found.

Virus detection software running in "active mode" refers to software that performs its desired function automatically. With active virus detection software, workstations continually monitor themselves for the presence of viruses or virus-like behavior.

The following guidelines govern all workstations connected to the District network:

- All workstations must have virus detection software installed in active mode.
- Workstations may be scheduled for periodic hard drive anti-virus scans by the system administrator.
- All software must be screened and verified by active virus detection software before being loaded.

Upon discovery or suspicion of a virus, the workstation user must:

- Cease all operations.
- Notify the building technology liaison or Information Technology Services Department.
- Immediately isolate any affected system.
- Document conditions and status of the environment.

Software

Copyright laws protect most software programs. Unauthorized copying is a violation of Federal Law and District Copyright Policy 2025. By using District provided software, users agree to abide by any and all licensing agreements. The District is subject to random license audits by software vendors and/or their agents. Users who install unauthorized software may be held personally liable for any copyright and licensing infringement including fines and/or disciplinary action. The Director of Information Technology Services, or designee, reserves the right to restrict the installation of software, and remove unlicensed or non-standard software.

Instructional software must be reviewed in accordance with building-level and District-level Instructional Materials Committee guidelines.

Records Retention

All files and electronic mail on the System are subject to disclosure under the Request for Public Records policy and RCW 42.17. The District reserves the right to retain or destroy records concerning any use of the System.

Users are responsible for knowing and abiding by state records retention guidelines as published by the Secretary of State for school districts. The following categories of electronic communication usually meet public records requirement:

- Policy and Procedure Directives
- Correspondence or memoranda related to official public business
- Agendas and minutes of meetings
- Documents relating to legal or audit issues
- Messages which document agency actions, decisions, operations and responsibilities
- Documents that initiate, authorize or complete a business transaction
- Drafts of documents that are circulated for comment or approval
- Final reports or recommendations
- Appointment calendars
- E-mail distribution lists
- Routine information requests

- Other messages sent or received that relate to the transaction of local government business

Souce: GENERAL RECORDS RETENTION SCHEDULE FOR SCHOOL DISTRICTS AND EDUCATIONAL SERVICE DISTRICTS IN WASHINGTON STATE, March 27, 2003

Diligent effort must be made to conserve System resources including removal of old email and computer files not subject to the Request for Public Records policy.

For security and administrative purposes, the District reserves the right to have authorized personnel (i.e., the System Administrator or designee) review System use and file content and to copy System files, including, without limitation, the contents of email messages and all files downloaded or stored on District computers or equipment.

District Web Site

The purpose of the District web site is to disseminate appropriate information to staff or students and to provide information for parents and the community.

The Communications and Community Relations Department is responsible for the overall structure of the South Kitsap School District web site and must insure compliance with all Federal and State law, District policy and regulations (technology ethics), and administrative directives. Communications and Community Relations staff is also responsible for training building and department web managers and must keep all completed Web Manager Publication Agreements on file.

Building principals and department directors are responsible for all content posted on their building/department site and must assure compliance with all Federal and State law, District policy and regulations (technology ethics), and administrative directives.

Each building principal and department director may designate a person who will serve as their own web manager. They will be responsible for all content posted on their building/department site and must assure compliance with all Federal and State law, District policy and regulations (technology ethics), and administrative directives.

Each web manager will receive training by the Communications and Community Relations Department before they have access to the web page. Web managers are also responsible for keeping Release of Personal Information forms for students and staff at their building or department.

The South Kitsap School District web publishing capabilities are for educational use only. All documents published on the SKSD website represent the District and, as such, should reflect professionalism and educational relevance.

No links to sites filtered by the SKSD web filtering system are permitted.

No student address information may be posted on the web site or be embedded in the underlying code. Address information includes: address, phone number, student ID, Social Security number and student email address.

Student photographs, first name and last initial, and age may appear on a web page only with prior completion of the Release of Personal Information for Student form by parent or guardian. These forms are only considered valid while a student is enrolled in his/her school. As a student moves between schools, a new form must be completed and housed at their new school. *See the Student Release of Personal Information form.*

Club and team photographs, article bylines, student election information, and students involved in learning activities are all examples of appropriate use. Individual class photos, electronic yearbook photos, and photos without a specific academic purpose should not be used.

All student produced web pages must be reviewed and posted by a faculty advisor or other web manager as designated by the building principal or department director. No student is permitted to post web pages to a public SKSD server.

Staff produced web pages must be reviewed and approved by the building principal or department director before being posted on the World Wide Web.

The www.skitsap.wednet.edu website is the official website for the District, including all schools and departments. No other school or department produced sites are allowed under any other address unless approved by the Director of Community Relations.

Violations

The Director of Information Technology Services shall report all incidents of inappropriate student use to the student's principal. The director of Information Technology Services shall report all incidents of inappropriate staff use to the staff member's supervisor and/or the Assistant Superintendent for Personnel and Labor Relations.

Disciplinary action, if any, for students, staff or other users shall be consistent with the District/school standard practices.

Costs incurred for investigation of misconduct may be passed on the user. Costs may include labor (including overtime and/or administrative overhead) and supplies for completing the investigation.

Communications, Training and Awareness

In lieu of a signed acceptable use form, the District shall, at the beginning of each school year, communicate with staff, parents and students the key principles of this policy and procedure, specifically:

- Personal safety while using the internet, including keeping passwords confidential;
- Consequences of accessing inappropriate web sites and bypassing security;
- Copyright and fair use guidelines;
- Cyber-bullying signs and reporting process;
- Public records compliance (for staff).

The format of communication for staff should be the annual review of the procedures during a staff meeting.

The format of communication for students and parents shall include an informational letter/brochure that outlines the District's expectations alongside tips for parents to use with students at home. Where available, this information should be included in District provided student handbooks/planners as the primary communication method.