AR-4119.26 (a)
AR-4219.26 (a)
AR-4319.26 (a)

EMPLOYEE TECHNOLOGY USAGE

I. APPROPRIATE USES

As with any other equipment provided by the district, technology is provided in order to further the district's educational and operational purposes.

Staff personal use of technology that is consistent with the district's educational mission may be permitted at times when it will not interfere with the staff member's employment responsibilities, when authorized by the staff member's immediate supervisor or other appropriate administrator.

All users of the Internet and the district's internal computer systems (intranet), must abide by generally accepted rules of network etiquette or "netiquette." These include, but are not limited to, the following:

a) Be polite. Do not be rude or abusive towards or about anyone, regardless of whether or not they are the recipients of a message or file;

b) Use appropriate language. Do not swear or use vulgarities. Avoid using all capital letters since it indicates shouting.

c) Keep personal information confidential, except where its release is specifically authorized.

d) Do not use any of the district's technology in a way that could disrupt use by others.

In addition to any other uses that are not appropriate or which would violate the guidelines in these regulations, the district strictly prohibits and will not tolerate any use of its technology for activities related to the

a) violation of any local, state or federal law;

b) access, receipt, display or transmittal of any pornographic or lewd information or access by minors of any material that is harmful to minors, as that term is defined in the Children's Internet Protection Act;

AR-4119.26 (b)
AR-4219.26 (b)
AR-4319.26 (b)

EMPLOYEE TECHNOLOGY USAGE (continued)

c) access, receipt, display or transmittal of any information pertaining to the construction, manufacture or use of weapons, injurious devices, or toxic, poisonous or injurious substances except in the context of an approved educational or operational activity;

d) participation in or organization of gambling;

e) solicitation of or transaction of personal business during the employee's working hours, or other profit-making activity, except in the context of an authorized educational activity;

f) promotion of local, state, or national political causes or candidates;

g) promotion of religion or religious activities;

h) harassment, cyber bullying or threatening of any individual;

i) release of personally identifiable information about a student in violation of the district's student records policy and regulations;

j) unauthorized access of digital files or systems, whether internal or remote;

k) destruction or deletion of district, school or student-related records, files, e-mail or programs without supervisor approval;

The prohibitions regarding political and religious speech contained in subsections f) and g) above are not intended to restrict personal, non-harassing speech that is protected by the First Amendment. They are intended solely to prevent speech that is school-sponsored or communicated under circumstances that give the appearance of school sponsorship, and to prevent district resources from being used unlawfully to support political or religious causes. Where access to district technology resources is provided to student groups, it shall be provided consistent with the requirements of federal laws relating to equal access.

AR-4119.26 (c)
AR-4219.26 (c)
AR-4319.26 (c)

EMPLOYEE TECHNOLOGY USAGE (continued)

II. ACTIVE SAFETY MEASURES

The district will use filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors. The district will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material that is inappropriate for minors.

Internet filtering software or other technology-based protection systems may be disabled by a school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 17 or older.

The term "harmful to minors" is defined by the Children's Internet Protection Act as meaning any picture, image, graphic image file, or other visual depiction that

- taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
- depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
- taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Staff shall be directed to caution students against disclosing their last names or other personal information that might allow a person to locate them to anyone with whom the students are communicating via the Internet unless they first obtain the permission of their supervising teacher. Students should also be cautioned against arranging face-to-face-meetings with individuals they have "met" only online unless they have their parents' permission, and should be cautioned against meeting individuals whom they have previously communicated with only online in a secluded place or private setting.

Staff members shall not publish photographs of students without signed permission of the parents and permission from the building administrator.

It is the responsibility of the employee to change default passwords for school email accounts and other electronic systems and software immediately upon receipt of a default password. Passwords should be kept in a secure location and not shared with others. Passwords should be updated regularly, at a minimum every two years.

AR-4119.26 (d)
AR-4219.26 (d)
AR-4319.26 (d)

EMPLOYEE TECHNOLOGY USAGE (continued)

III. PROTECTING AGAINST HARM TO THE TECHNOLOGY

Technology of any kind is fragile and sensitive to disruption and destruction for many reasons. It is the responsibility of all users to exercise caution and to take affirmative steps to protect the security and integrity of the district's technology.

The district is particularly concerned about the introduction of damaging viruses and malware/adware. Such viruses and malware/adware can be transmitted easily and in a number of different ways. Users may be liable for any damage caused to the district's technology if they fail to follow the precautions described in this policy.

It is a violation to purchase, download, install or use software, hardware, applications and/or peripherals on district equipment and networks that have not been expressly approved by the technology director. This authorization is also required before using any electronically readable devices not provided by the district or before transferring any files over the Internet or by any other means. For all technology related purposes, a copy of the license agreement should be forwarded to the Technology Director for tracking and audit purposes.

The District reserves the right to use simulated digital attacks to help train staff.

IV. PROHIBITION OF ANY INFRINGEMENTS TO INTELLECTUAL PROPERTY RIGHTS

Users are responsible for assuring that none of their uses of the district's technology could in any way violate applicable copyright, trademark or patent laws. In general, before duplicating any software, users must obtain the express written consent of its publisher.

Unauthorized duplication of the district's software is strictly prohibited. Users will be liable for any damages caused by their infringement of the intellectual property rights of others.

V. PERSONAL TECHNOLOGY BEHAVIORAL EXPECTATIONS

Anyone who brings a privately-owned device to Wrangell Public Schools is personally responsible for the equipment. Responsibility for the maintenance and repair of the equipment rests solely with that individual, including installation of software and configuration of peripherals. Any damage to the equipment, including results from viruses, is the responsibility of the individual.

AR-4119.26 (e)
AR-4219.26 (e)
AR-4319.26 (e)

EMPLOYEE TECHNOLOGY USAGE (continued)

Software residing on privately-owned devices must be personally owned unless authorized by the district and within the licensing constraints of the software company. The district retains the right to determine where and when privately-owned equipment may be attached to the network. The individual is responsible for the security of the equipment at all times.

A privately-owned device may be allowed connection to the district's network, including access to the Internet, under the following conditions:

- Use of the device must adhere to Wrangell Public Schools' policies and procedures.
- File storage on the network from privately-owned devices is limited to official business only.
- The individual must supply all necessary hardware/software and cabling to connect to the network.
- Prior to connecting to the district network or Internet the user of a privately-owned device must take appropriate action to prevent malware on the device. This may include running anti-virus software and/or keeping security software up to date.
- The individual has a signed Acceptable Use Agreement for Employees form on file.

Even in circumstances where personal technology use is permitted at work, the viewing of sexually explicit or offensive material, or any material that is contrary to Wrangell Public Schools' Mission, Vision and Values or our board policy is strictly prohibited.

Ringers/alerts on personal technology should be silenced during working time and while in the classroom unless authorized by the administration.

There can be no expectation of privacy on any device used in the district, including privately-owned devices.

As it relates to privately-owned devices being used in district facilities, the district reserves the right to:

- Monitor and log all activity,
- Make determinations on whether specific uses of the device are consistent with the district's policies and procedure,

AR-4119.26 (f)
AR-4219.26 (f)
AR-4319.26 (f)

EMPLOYEE TECHNOLOGY USAGE (continued)

• Deem what is appropriate and inappropriate,

• Restrict access to district resources, such as printers and servers,

• Remove the user's access to the network and suspend the right to use the privately-owned device in district facilities at any time if it is determined that the users are engaged in unauthorized activity or are violating district policies and procedures.

Electronic messages on personal technology (for example emails or text messages), even those that have been deleted, are typically discoverable in legal proceedings to the same extent as hard copies. By transmitting a message electronically, a user may be deemed to have waived certain privacy protections that would otherwise be available.

Disciplinary action for misuse of privately-owned devices at district facilities shall be consistent with the district's policies and procedures. Violations may be cause for removing the individual's access privileges, suspension of use of the privately-owned device in district facilities and other disciplinary actions and/or appropriate legal action.

VI. SOCIAL MEDIA BEHAVRIORAL EXPECTATIONS

Whether you are posting for business or personal reasons, the following are expected of all staff members.

- Always act consistently with Wrangell Public Schools' Mission, Vision & Values and our school board policies.
- Know and follow laws, regulations and Wrangell Public Schools policies regarding privacy and confidentiality at all times.
- Always be aware that written messages are, or can become, public. The Internet is immediate and nothing posted is ever truly private or anonymous.
- If a staff member sees unfavorable opinions, negative comments or criticism about Wrangell Public Schools on a social media site, he or she should not attempt to rebut it nor have it removed as that may escalate the situation. Instead, he or she should forward the information to the Superintendent.
- Any staff member who believes they have been the target of harassment through another staff member's social media activity should report the incident to their supervisor. Abusive or harassing behavior violates Wrangell Public Schools' policy and is subject to disciplinary action, up to and including termination of employment.

EMPLOYEE TECHNOLOGY USAGE (continued)

- Any unauthorized information posted on a social media site that discloses confidential or proprietary Wrangell Public Schools information or implies official Wrangell Public Schools opinion violates Wrangell Public Schools' policy and may be used as grounds for discipline, up to and including termination, even if the action was on personal time and equipment.
- A suspected Breach of Confidentiality will be dealt with according to Wrangell Public Schools' Confidentiality policy.
- Wrangell Public Schools administration has the right to view, monitor and request removal of any posting on a social media site that does not meet the requirements of this regulation.

VII. CONFIDENTIALITY, SECURITY AND REPRESENTATIONS

The district is concerned with the risk of release of confidential or sensitive information and access to its systems by unauthorized persons. The district is also concerned with liabilities that could result from its misrepresentation on the Internet or through other electronic communications.

Users shall not disclose any confidential information to unauthorized persons. This specifically includes confidential educational and personnel records.

Users should not disclose their password, user identification information, or remote access information to anyone except the network administrator, or allow others to use their accounts or passwords without the approval of the network administrator, superintendent or superintendent's designee. Users shall not impersonate another user, or use another's password or account unless such use is approved by the network administrator, superintendent or superintendent's designee. Users who discover any actual or potential security problem or release of confidential information should report it immediately to the network administrator, superintendent or superintendent's designee.

In addition, users must be cautious not to use the district's technology to broadcast or in any way distribute statements on the Internet or elsewhere that could be understood by others to be representations by the district unless such statements are specifically authorized by the superintendent or superintendent's designee.

AR-4119.26 (h)
AR-4219.26 (h)
AR-4319.26 (h)

EMPLOYEE TECHNOLOGY USAGE (continued)

VIII. NO EXPECTATION OF PRIVACY

Users should not expect privacy in any of their uses of the district's computer technology. In the normal course of operations, the district routinely logs, retains and stores data that record the contents of electronic mail messages received to and from all employees/students, documents produced by students/employees, and information accessed over the Internet or through any other means.

Information that users may have deleted may not be eliminated fully from the computer system. Users should assume that there exists a permanent record of everything that they do involving the district's technology. Maintenance, installation of upgrades, and other such activities within the district's normal course of operations may reveal the contents of information contained in the technology and its systems.

In addition, the district, in its sole discretion, may monitor and review any user's use of its technology in order to assure compliance with this or any other of the district's policies. The district, including its contracted affiliates, need not provide users with any further notice before it monitors, reviews, copies or stores any information that users may have received, transmitted, created or stored while using any of the district's technology.

IX. CONSEQUENCES FOR VIOLATION OF THE POLICY

Failure to comply with these regulations could result in the temporary or permanent revocation of the privilege to use the district's technology. It could also subject offenders to discipline up to and including termination from employment.

In the event that a user's violation of this policy causes damage to any district property or the incursion of any liability by the district, the user may be held personally liable for the damage or costs incurred by the district.

AR-4119.26 (i)
AR-4219.26 (i)
AR-4319.26 (i)

EMPLOYEE TECHNOLOGY USAGE (continued)

X. PURCHASE OF DISTRICT TECHNOLOGY UPON RETIREMENT/SEPARATION

Employees who have **five years** of continuous service with Wrangell Public Schools may be eligible to purchase a district device that has fulfilled its service lifetime with the district. The following value depreciation scale will be used when selling district technology, unless value is otherwise determined by the Technology Director:

3-year old device	cost less 50%
4 or 5-year old device	cost less 75%
Over 5 years old	$50.00

Technology devices under 3-years old will not be offered for sale to employees at retirement or separation from the district..

Adoption Date:	January 14, 2002
Revised and Renumbered in Consultation with Legal Counsel:	June 10, 2011
Reviewed in Consultation with Legal Counsel:	August 8, 2011
Reviewed:	February 18, 2013
Revised:	April 24, 2017
Revised:	August 19,2019
Reviewed:	November 18, 2024
Revised:	November 19, 2025