**Electronic Information System (K-20 Network) Policy**

Every Eastmont School District employee is responsible for using the electronic mail (e-mail) system properly and in accordance with this policy. Any questions about this policy should be addressed to the Director of Technology and/or the Executive Director of Human Resources.

The e-mail system is the property of Eastmont School District. It has been provided by public dollars through the Office of the Superintendent of Public Instruction (OSPI) for use in conducting agency business. All communications and information transmitted by, received from, or stored in this system are agency documents and accessible by the public. The e-mail system is to be used for agency purposes only. Use of the e-mail system for personal purposes is prohibited.

ELECTRONIC INFORMATION SYSTEM (K-20 NETWORK)

Policy No. 2022

The Board of Directors recognizes that the district is connected to a statewide communications system (the K-20 Network) which provides Internet access and interactive video conferencing. This network allows unprecedented opportunities for students, staff and patrons to communicate, learn, access, and publish information. The Board believes that the resources available through this network and the skills that students will develop in using it are of significant value in the learning process and student success in the future. These new opportunities also pose many new challenges including, but not limited to, access for all students, age-level appropriateness of material, conservation of resources, security/privacy/confidentiality, and cost of maintaining the system. The district will endeavor to ensure that these concerns are appropriately addressed, but cannot insure that problems will not arise.

By connecting to this network, the Board intends only to provide a means for educational activities and does not intend to create a first amendment forum for free expression purposes. The district dedicates the property comprising the network, and grants access to it by users, only for the educational activities authorized under this policy and procedures and under specific limitations contained therein.

The Board directs the Superintendent to provide training and procedures that encourage the widest possible access to the K-20 network by students, staff and the educational community, while establishing reasonable controls for the lawful, efficient and appropriate use and management of the system.

Eastmont School District Network (ESDN) and

K-20 Network Acceptable Use Guidelines/Internet Safety Requirements

### General Use

1. No person shall have access to the K-20 Network without having received appropriate training, and a signed Individual User Release Form must be on file with the district. In addition, students under the age of 18 must have the approval of a parent or guardian.
2. Nothing in these regulations is intended to preclude the supervised use of the network while under the direction of a teacher or other approved user acting in conformity with district policy and procedure.
3. Any violation of the requirements of this policy, procedure, or any other student or employee conduct rules applicable to the use in question may subject the user to student disciplinary action or personnel disciplinary action up to and including suspension or expulsion of students or termination of employment.
4. The system administrators of ESDN reserve the right to suspend or permanently remove users access to the system if at any time it is determined that the user has violated one or more standards contained in Eastmont School District Procedure No. 2022P Network Acceptable Use Guidelines. A user’s right to access the system shall not be denied or removed without just cause.
5. Maintaining or posting material to a web site or blog that threatens a likelihood of a substantial disruption in school, including harming or interfering with the rights of students to participate fully in school or co-curricular activities is a violation of the student disciplinary code and subject to appropriate penalties herein.
6. All student use of the District Internet system or personal cell phones or other digital devices used by students while on campus is subject to the provisions of the Disciplinary Code. Students may not share or post personal information about or images of any other student or staff member without permission from that student or staff member. Violations of this policy may result in loss of all use of a personal cell phone, network access, and other disciplinary consequences.
7. Diligent effort must be made to conserve system resources. For example, users should frequently delete E-mail and unused files, and users should promptly disconnect videoconferences on completion.
8. No personal computers may be used on ESDN.
9. No donated equipment shall be accepted without prior approval from the district Technology Director.

### Network Use

1. All use of the system must be in support of education and research and consistent with the mission of the district. The district reserves the right to prioritize use and access to the system.
2. Any use of the system must be in conformity to state and federal law, K-20 Network policies, and district policy. Use of the system for commercial or personal solicitation is prohibited.
3. The system constitutes public facilities and may not be used to support or oppose political candidates or ballot measures.
4. No use of the system shall serve to disrupt the operation of the system by others; system components including hardware or software shall not be destroyed, modified, or abused in any way.
5. Malicious use of the system to develop programs or institute practices that harass other users or gain unauthorized access to any entity on the system and/or damage the components of an entity on the network is prohibited.
6. Users are responsible for the appropriateness of the material they transmit over the system. Hate mail, harassment, discriminatory remarks, or other antisocial behaviors are expressly prohibited.
7. Use of the system to access, store, or distribute obscene or pornographic material is prohibited.
8. Staff - Subscriptions to mailing lists, commercial on-line services and other information services must be for job related purposes.
9. Staff -Use of blogs, wikis, email, chat, instant messaging and other forms of internet communication must be for the purpose of job related professional use only. Use of such services may require a change to ESDN’s filtering software.
10. Students - Use of blogs, wikis, email, chat, instant messaging and other forms of internet communications are prohibited.

### Security

1. ESDN logins or accounts are to be used only by the authorized owner of the account for the authorized purpose. Users may not share their account number or 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.
2. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users; misrepresent other users on the system; or attempt to gain unauthorized access to any system.
3. The district has the right to review or remove materials installed, used, stored, or distributed on or through the network without notice. There should be no expectation of privacy.
4. Users should change passwords regularly and avoid easily guessed passwords.

### Personal Security

1. Personal information such as complete names, addresses, telephone numbers and identifiable photos should remain confidential when communicating on the system. Students should never reveal such information without permission from their teacher and parent or guardian. No user may disclose, use, or disseminate personal identification information regarding minors without authorization.
2. Students should never make appointments to meet people in person whom they have contacted on the system without district and parent permission.
3. Students should notify their teacher or other adult whenever they come across information or messages they deem dangerous or inappropriate on the web.

Filtering and Monitoring

1. The District has implemented a filtering solution designed to comply with CIPA (Children’s Internet Protection Act) guidelines. The following categories are currently being filtered at all grades: gambling, criminal skills, hate speech, violence, weapons, drugs, alcohol and tobacco, hacking, adult/sexually explicit, glamour & intimate apparel, personals & dating, remote proxies, sex education, usenet news, chat, web-based email, streaming media, photo searches and hosting sites.
2. Process for review of filtered content – In the likely event that content needs to be added to or removed from the list of filtered Internet sites, a request for review should be submitted to the district Technology Director or designee, which will be charged with the responsibility to review any additions or deletions and make appropriate changes.
3. Educational staff will, to the best of their ability, monitor minors’ use of the Internet in school, and will take reasonable measures to prevent access by minors to inappropriate material on the Internet and World Wide Web, and restrict their access to materials harmful to minors.

### INTERNET SAFETY

### Web

The district will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district computers by employees assigned to supervision of specific students.

1. Documents shall include only the first name of the student.
2. Documents shall not include a student’s home phone number, address, or names of other family members or friends.
3. Student projects, student work, classroom activities and school activities may be displayed on the District website. Only relevant information will be published, which may include a student’s first name, photograph, short audio and or video clips.
4. No student work shall be published without permission of the student and parent or guardian.

### Web Sites

1. Material placed on web pages is expected to meet academic standards of proper spelling, grammar and accuracy of information.
2. Material (graphics, text, sound, etc.) that is the ownership of someone other than staff or students may not be used on Web sites unless formal permission has been obtained.
3. All Web pages should have a link back to the home page of the classroom, school or district, as appropriate.

### Videoconference

1. Videoconferencing is a way that students and staff can communicate with other students, staff, classrooms, speakers, museums, etc. from other parts of the country and the world. With videoconferencing equipment, students can see, hear, and speak with other students, speakers, museum personnel, etc. in real-time.
2. Videoconference sessions may be videotaped by district personnel or by a participating school involved in the exchange in order to share the experience within ours or their building or district.
3. Students’ voices, physical presence, and participation in the videoconference are transmitted to participating sites during each session. Rules and procedures relative to acceptable use and behavior by students and staff apply during all videoconference sessions.

### Copyright

The unauthorized installation, use, storage, or distribution of copyrighted software or materials on district computers is prohibited. All users of the K-20 Network shall comply with current copyright laws.

### Email

1. Student: Email is not provided for students as part of their enrollment at Eastmont.
2. Staff: Every ESDN user who has an email account is responsible for using the electronic mail (email) system properly and professionally.
3. Employees have no right of personal privacy in any matter stored in, created, received, or sent over ESDN mail system.
4. Eastmont School District, in its discretion as owner of the email system, reserves and may exercise the right to monitor, access, retrieve, and delete any matter stored in, created, received, or sent over the email system, for any reason and without the permission of any employee without notice.
5. Eastmont School District has the right to retrieve and read any email messages. Those messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any email messages that are not sent to them. Any exception to this policy must receive the prior approval of the Superintendent. Access may be granted for compliance purposes, regulatory purposes, law enforcement purposes, or other legitimate purposes.
6. Email records and computer files may be subject to discovery in litigation, Eastmont employees are expected to avoid making statements in email or computer files that would not reflect favorably on the employee or Eastmont School District if disclosed in litigation or otherwise.

### Voice Mail

1. Every ESDN user who has a voice mail account is responsible for using the Voice Mail system properly and professionally.
2. The Voice Mail system is the property of Eastmont School District. It has been provided by Eastmont for use in conducting school business. All communications and information transmitted by, received from, or stored in this system are property of Eastmont School District. Use of the Voice Mail system for personal purposes is prohibited.

### Software

Software installation must be completed by a district technology staff member or other approved individual. All installed software must be properly licensed. Students are prohibited from installing software on any district computer unless they have prior approval from the district Technology Director or designee. Additionally, downloading and/or storing executable files (programs) are prohibited.

### Personal Electronics

1. All personal network related electronics located on school grounds shall have a form on file with designated building contact and District Technology Department stating: make, model, serial number and staff name.
2. The district cannot provide service or support for personal equipment.
3. The district cannot provide replacement parts for personal equipment.

From time to time, the district will make a determination on whether specific uses of the K-20 Network are consistent with the regulations stated above. Under prescribed circumstances non-student or staff use may be permitted, provided such individuals demonstrate that their use furthers the purpose and goals of the district. For security and administrative purposes the district reserves the right for authorized personnel to review network use and content. The district reserves the right to remove an individual’s network access privileges to prevent further unauthorized activity. Violation of any of the conditions of use may be cause for disciplinary action, up to and including termination.

GENTLE REMINDERS

E-Mail

* No expectation of privacy; the District retains the right to review, audit, intercept, access, and disclose all material created, received, or sent over the network system.
* Do not use the District e-mail system for personal gain or solicitation, (i.e. giving away or selling of personal items, etc.)
* Do not open any e-mails or attachments from unknown origins.
* Do not e-mail/share software or other copyrighted material.
* Do not pass on jokes, advertisements, or other messages that may be considered chain or junk mail.

Internet

* At all levels, use of the Internet should be purposeful and integrated into the curriculum.
* Each school will be responsible for determining how students will receive training for the Internet.
* Be aware of and abide by copyright and licensing laws.
* Monitor student activity while using district equipment. Notify building administration of any inappropriate activity.
* Do not use the Internet for commercial purposes.
* Do not use the Internet to access or process pornographic or otherwise inappropriate material.
* Protect your network login information (login name and password).
* Notify network administrators if your personal information has been compromised.
* Do not leave your workstation unattended when logged onto the system. Log off the Internet/Network as soon as you have completed your work.

STUDENT COMPUTER ESSENTIALS

General Guidelines

Use of the Internet by students and staff of Eastmont School District shall be in support of education and research that is consistent with the mission of the district. Internet use is limited to those persons who have been issued district approved accounts. Use will be in accordance with the district’s Acceptable Use Procedures and this Code of Conduct.

1. Always have staff supervision when using the Internet.
2. Never give out your name, address, age, date of birth, sex or any other personal information.
3. Protect your internet logon information. (LOGON NAME and PASSWORD)
4. Notify network administrators if your personal information has been compromised.
5. Downloading of ANY content without permission is against district policy, (i.e. programs, games, graphics, mp3 music, videos etc.).
6. Treat information created by others as the private property of the creator.
7. Use the network in a way that does not disrupt its use by others.
8. Do not use or pass software that could damage the components of a computer or computing system, such as viruses, worms, chain messages, global mailings, etc… Do not attempt to “hack” the system.
9. Do not use the Internet to view or download pornographic or otherwise inappropriate material. If you find anything inappropriate, immediately inform a member of the staff.
10. Do not use the Internet for non-school related purposes.

The district reserves the right to remove a user’s account if it is determined that the user is engaged in unauthorized activity or is violating this code of conduct.

Appropriate Use of District Resources

The purpose of this policy is to ensure proper usage of Eastmont School District’s resources synonymous with state resources. An Eastmont School District employee may not use state resources for private benefit or gain of the officer, employee or another person.

The definition of “state resources” is all encompassing and includes, but is not limited to, office space, employee duty time, equipment, supplies, publications, mailing lists, and all forms of communications media including newsletters, e-mail, faxes, and telephones, etc.

State resources are to be used for Eastmont School District business only. Employees who abuse this public trust may be subject to corrective or disciplinary action. The specific examples listed below are illustrative but not intended to be an all-inclusive list:

1. Office telephones are for official use. Local personal calls must be kept to a minimum and generally limited to emergency situations. Long distance calls are not authorized for personal use.
2. Cellular telephones are for official use. No personal calls are allowed except in emergency situations only.
3. SCAN authorization codes are to be used for official business only.
4. Eastmont School District vehicles are to be used by employees for official business only. Employees may transport only passengers who are on official state business.
5. Office stationery and other supplies are not for personal use.
6. Each employee is responsible for ensuring that personal mail is delivered to his or her home mailing address, not to the work location.
7. Copy machines, facsimile machine, printers, audio-visual equipment, computer hardware and software are to be used for official business only.
8. Only work-related software applications are appropriate on Eastmont School District computers.
9. Internet usage is limited to obtaining information related to the employee’s job or other tasks assigned by the supervisor.

Administrators may authorize, in advance, temporary exceptions for specific goals described in the employee’s Professional Growth Option.

RCW 42.52.16