ELECTRONIC RESOURCES AND INTERNET SAFETY

Acceptable Use Guidelines/Internet Safety Requirements

These procedures are written to support the Electronic Resources Policy of the Eastmont School District Board of Directors and to promote positive and effective digital citizenship among students and staff. Digital citizenship includes the norms of appropriate, responsible, and healthy behavior related to current technology use. Successful, technologically-fluent digital citizens recognize and value the rights, responsibilities, and opportunities of living, learning, and working in an interconnected digital world. They cultivate and manage their digital identity and reputation, and are aware of the permanence of their actions in the digital world. Expectations for student and staff behavior online are no different from face-to-face interactions.

Individual User Release Form

All users must have a signed Individual User Release Form before access to the District's network resources will be permitted. Staff must complete and submit 2022-F1 at the time of hiring. Students must complete 2022-F2 at the time of registering to attend school in the District. Students under the age of 18 must have the approval of a parent/guardian.

Use of Personal Electronic Devices

In accordance with all Eastmont School District policies and procedures, students and staff are issued District devices to further the educational mission of the District. School administration will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during the school day. Absent a specific and articulated need (e.g., assistive technology), students do not have an absolute right to possess or use personal electronic devices at school.

A. Students are required to use an Eastmont School District issued device to access digital content and curriculum while at school or offsite.

B. Personal laptops/computers/tablets are not permitted at school.
    1. Personal devices could circumvent student safety monitoring services (e.g., Gaggle), Classroom monitoring/management (e.g., Impero Classroom), and potentially web filtering.
    2. Exceptions may be granted by building administration for personal devices that require Wifi Access and Form 2022-F3 must be completed and signed by all parties.

C. Use of cell phones must follow School Board Policy No. 3245 Students and Telecommunication Devices

Network

The District network includes wired and wireless devices and peripheral equipment, files

and storage, email and Internet content (blogs, websites, collaboration software, social networking sites, wikis, etc.). The District reserves the right to prioritize the use of, and access to, the network.

All use of the network must support education and be consistent with the mission of the District.

Acceptable use of District technology resources by District staff and students include:

A. Creation of files, digital projects, videos, web pages, and podcasts using network resources in support of education and research;
B. District approved and supervised participation on websites that support education and research;
C. With parental permission, the online publication of original educational material, curriculum-related materials, and student work. Sources outside the classroom or school must be cited appropriately; and
D. Staff use of the network for incidental personal use in accordance with all District policies and procedures.

Unacceptable network use by District staff and students includes, but is not limited to:

A. Eastmont's general guideline for both staff and students uses old fashioned technology - the Newspaper Test. This means asking while they are using District technology if they would want whatever they are writing, viewing, or listening to go on the front page of the Wenatchee World Newspaper (or an online version). If not, then they should stop immediately. If there is a question about the use, they should ask a supervisor for guidance on appropriate use;
B. Personal gain, commercial solicitation, and compensation of any kind;
C. Accessing personal email or other personal accounts from a District owned device;
D. Logging into or using another person's account in any way;
E. Actions that result in liability or cost incurred by the District;
F. Users shall only use licensed and up to date software. Any installation must be completed by a District technology staff member or other approved individual.
G. Support for or opposition to ballot measures, candidates, and any other political activity;
H. Hacking, cracking, vandalizing, the introduction of malware, including viruses, worms, Trojan horses, time bombs, and changes to hardware, software, and monitoring tools;
I. Unauthorized access to other District computers, networks, and information systems;
J. Action constituting harassment, intimidation or bullying, including cyberbullying, hate mail, defamation, discriminatory jokes, and remarks. This may also include the

manufacture, distribution, or possession of inappropriate digital images;

K. Information posted, sent, or stored online that could endanger others (e.g., bomb construction, drug manufacturing);

L. Opening emails or attachments from unknown origins;

M. Emailing or sharing software or other copyrighted material or other violation of copyright laws;

N. Unauthorized installation, use, storage, or distribution of copyrighted software or materials is prohibited;

O. Accessing, uploading, downloading, storage and distribution of obscene, pornographic, or sexually explicit material;

P. Attaching unauthorized devices to the District network. Any such device will be confiscated and additional disciplinary action may be taken;

Q. Any unlawful use of the District network, including but not limited to stalking, blackmail, and fraud; or

R. Any activities that disrupt school or District activities.

The District will not be responsible for any damages suffered by any user, including, but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by his/her own negligence or any other errors or omissions. The District will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the District's computer network or the Internet.

Internet Safety/Personal Information and Inappropriate Content

A. Staff and students should not reveal personal information, including a home address and phone number on websites, blogs, podcasts, videos, social networking sites, wikis, email, or as content on any other electronic medium;

B. Staff and students should not reveal personal information about another individual on any electronic medium without first obtaining permission;

C. Student pictures or names cannot be published on any public class, school or District website unless the appropriate permission has been obtained according to Form 2022-F2;

D. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority immediately; and

E. Students should be aware of the persistence of their digital information, including images and social media activity, which may remain on the Internet indefinitely.

Filtering and Monitoring

Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered.

A. Filtering software is not 100 percent effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his/her use of the network and Internet and avoid objectionable sites;

B. Any attempts to defeat or bypass the District's Internet filter or conceal Internet activity are prohibited (e.g., proxies, https, special ports, modifications to District browser settings, and any other techniques designed to evade filtering or enable the publication of inappropriate content);

C. Email inconsistent with the educational and research mission of the District will be considered SPAM and blocked from entering District email boxes;

D. 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 devices;

E. Staff members who supervise students, control electronic equipment, or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the District

F. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct, and assist effectively;

G. The District may monitor student use of the District network, including when accessed on students' personal electronic devices and devices provided by the District, such as laptops, Chromebooks, and tablets; and

H. The District will provide a procedure for staff to request access to Internet websites blocked by the District's filtering software. The requirements of the 'Instructional Technology Approval Form' cover a wide criteria including compliance with federal regulations such as CIPA, COPPA, FERPA. As well as justification for how the website is supplemental to core instruction.

Internet Safety Instruction

All students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response:

A. Age appropriate materials will be made available for use across grade levels; and

B. Training on online safety issues and materials implementation will be made available for administration, staff, and families.

Copyright

Downloading, copying, duplicating, and distributing software, music, sound files, movies, images, or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. All use of any material other than approved curriculum in the classroom is the individual staff member's responsibility to verify that copyright guidelines are followed in duplication and distribution. Staff members must be

prepared to back up all duplication and distribution actions of outside material to District Administration upon notification.

Video Streaming services
Streaming services (Netflix, Disney+, Amazon Prime, Hulu, etc.) are blocked on Eastmont's network. The terms of service that one agrees to when purchasing the paid streaming service are for personal use only, not to be used in a public venue, including a classroom and would be a violation of those terms of service.

Ownership of Work
All work completed by employees as part of their employment will be considered property of the District. The District will own any and all rights to such work including any and all derivative works, unless there is a written agreement to the contrary.

All work completed by students as part of the regular instructional program is owned by the student as soon as it is created, unless such work is created while the student is acting as an employee of the school system or unless such work has been paid for under a written agreement with the school system. If under an agreement with the District, the work will be considered the property of the District. Staff must obtain a student's permission prior to distributing his/her work to parties outside the school.

Network Security and Privacy
Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account for authorized District purposes. Staff and students are responsible for all activity on their account and must not share their account password or leave an open file or session unattended. Account owners are ultimately responsible for all activity under their account.

The following procedures are designed to safeguard network user accounts:

A. Change passwords according to District policy;
B. Do not use another user's account;
C. Do not insert passwords into email or other communications;
D. If you write down your user account password, keep it in a secure location;
E. Do not store passwords in a file without encryption;
F. Do not use the "remember password" feature of Internet browsers;
G. Notify network administrators if your personal information has been compromised;
H. Users shall not seek information on, obtain copies of, modify files, data, or passwords belonging to other users, or misrepresent other users, or attempt to gain unauthorized access to any system; and
I. Lock the screen or log off if leaving a computer.

Student Data is Confidential
District staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).

No Expectation of Privacy
The District provides the network system, email, and Internet access as a tool for education and research in support of the District's mission. The District reserves the right to monitor, inspect, copy, review, and store, without prior notice, information about the content and usage of:

A. The District network, including when accessed on students' personal electronic devices and on devices provided by the District, such as laptops, netbooks, and tablets;
B. User files and disk space utilization;
C. User applications and bandwidth utilization;
D. User document files, folders and electronic communications;
E. Email;
F. Internet access; and
G. Any and all information transmitted or received in connection with network and email use.

No student or staff user should have any expectation of privacy when using the District's network. The District reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All content is subject to the public records disclosure laws of the State of Washington.

Educational Applications and Programs
District staff may request access for students to be able to access/sign up for websites, applications or programs that are used on District issued Chromebooks. Such applications and programs are designed to help facilitate lectures, student assessment, communication, and teacher-student feedback, among other things.

Students are required to use a District issued device to access digital content and curriculum while both at school or offsite.

Prior to requesting that students be given access to or sign up for educational applications or programs, staff will review "terms of use," "terms of service," and/or "privacy policy" of each application or program to ensure that it will not compromise students' personally identifiable information, safety, and privacy. Staff will also provide notice in writing of potential use of any educational application or program by completing the Instructional Technology Approval Form, including the anticipated purpose of such application or program. The Instructional Technology Approval Form must be signed by the staff member, their Principal/Director, the Executive Director of

Teaching and Learning as well as the Director of Technology.

Once a website or application has been reviewed and approved via the Instructional Technology Approval Form it will be added to a list of approved sites. Parents/ guardians are not directly notified of each approved application, but a list can be provided upon request.

Archive and Backup
Backup is made of all District email correspondence for purposes of public disclosure and disaster recovery. Barring power outage or intermittent technical issues, staff and student files are backed up on District servers regularly.

Disciplinary Action
All users of the District's electronic resources are required to comply with the District's policy and procedures (and agree to abide by the provisions set forth in the District's user agreement). Violation of any of the conditions of use explained in the District's user agreement, Electronic Resources policy, or in these procedures could be cause for disciplinary action, including suspension or expulsion from school and suspension or revocation of network and computer access privileges.

Accessibility of Electronic Resources
Federal law prohibits people, on the basis of disability (such as seeing and hearing impairments), from being excluded from participation in, being denied the benefits of, or otherwise being subjected to discrimination by the District. To ensure that individuals with disabilities have equal access to District programs, activities, and services, the content and functionality of websites associated with the District should be accessible. Such websites may include, but are not limited to, the District's homepage, teacher websites, District-operated social media pages, and online class lectures.

Allowed District Communication Methods in alignment with Procedure No. 4040-P
District staff with authority to create or modify website content or functionality associated with the District will take reasonable measures to ensure that such content or functionality is accessible to individuals with disabilities. Any such staff member with questions about how to comply with this requirement should consult with the District Technology Department.

All work and District related digital media accounts shall be approved by the employee's supervisor. Staff access to each respective Social Media account will be granted by social@eastmont206.org after building/department Admin approval. Parents/guardians shall also be provided access to digital communications that include their students.

Eastmont limits employees to the following communication technologies for District related communications:

A. District approved/monitored Google Gmail for email.
B. District approved/monitored Google Chat and Webex messaging for supervisor initiated texting.
C. District issued cell phones/District approved apps for texting.
D. District approved/monitored ParentSquare accounts.
E. District approved/monitored Facebook accounts.
F. District approved/monitored Twitter accounts.
G. District approved/monitored YouTube accounts.
H. District approved/monitored Instagram accounts.
I. District approved/monitored Pinterest accounts.
J. Other District Executive Administration approved social media accounts.
K. Student instruction or classroom related online accounts are prohibited due to the Family Educational Rights Privacy Act (FERPA) except if approved by the responsible supervisor and executive director.

Care for District Technology

No donated equipment shall be accepted without prior written approval from the Director of Technology.

Users of District technology are expected to respect the District's property and be responsible in use of the technology. Users are to follow any District instructions regarding maintenance or care of the technology. Users may be held responsible for any damage caused by negligent acts while District technology is under their control. The District is responsible for any routine maintenance or standard repairs to District technology. Recommendations for the care and cleaning of technology can be found on the Technology webpage. Users are expected to notify the District of any need for service in a timely manner.

Student technology (Chromebooks) are the responsibility of the student. If damage is caused negligently, a fee/fine will be issued via IIQ (Incident IQ). The fee/fine will then be reported to the parent/guardian via Intouch Receipting.

If District technology is lost, damaged, or stolen while under the control of a user, the user (or responsible parent/guardian if the user is a student) is expected to pay the fee/fine in a timely manner. The user is encouraged to file a claim under his/her homeowner insurance coverage to recoup the expenditure, when coverage is available.

Eastmont School District shall not be liable for any direct or indirect, incidental or consequential damages (including lost data or information) sustained or incurred in

connection with the use, operation, or inability to use Eastmont's network and/or devices, Violations of District policies or rules may result in appropriate disciplinary action up to and including termination.