Guidelines for Acceptable Use of Technology Resources (Student)

The Evergreen Public Schools (EPS) recognizes that an effective public education system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The district believes that students need to be proficient and safe users of information, media, and technology to succeed in a digital world.

Therefore, the district will use electronic resources as a powerful and compelling means for students to learn core subjects and applied skills in relevant and rigorous ways. It is the district's goal to provide students with rich and ample opportunities to use technology for important purposes in schools just as individuals in workplaces and other real-life settings use these tools. The district's technology will enable educators and students to communicate, learn, share, collaborate and create; to think and solve problems; to manage their work; and to take ownership of their lives and information.

To help ensure student safety and digital citizenship in online activities, 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.

1.0 User Responsibilities

1.1 It is expected that students will use electronic resources provided by the Evergreen Public Schools in study when using the district's internet and network. However, the failure of a student, or any other person to comply with these procedures while using the district's electronic resources may result in restricted access up to and including a complete denial of access.

1.2 All use of the electronic resources must be consistent with the mission and objectives of the Evergreen Public Schools, further district goals established by the board of directors, and in compliance with district policy and procedure.

1.4 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential Evergreen Public Schools information. Passwords must not be inserted into email messages or other forms of electronic communication. Passwords must not be revealed over the phone to anyone. Do not reveal a password on questionnaires or security forms. Do not share passwords with anyone, including family members. Do not write passwords down and store them anywhere. Do not store passwords in a file on a computer system or mobile device (phone, tablet) without encryption. Do not use the "Remember Password" feature of applications (for example, web browsers). Any user suspecting his/her password may be comprised must report the incident to the IT Service Desk (formerly Help Desk) and change all passwords.

1.5 District-owned devices must not be shared with any users not approved by Evergreen Public Schools. When sharing a device with other authorized users, log off of the device first.

2.0 Digital Citizenship

Digital Citizenship is the concept of educating all students in the appropriate use of technology. A good digital citizen is one who knows what is right and wrong, exhibits intelligent technology behavior, and makes good choices when using technology. All students are expected to abide by the generally accepted rules of network etiquette and conditions of Good Digital Citizenship. These include, but are not limited to:

2.1 **Respect Yourself**. Select online names that are appropriate, and consider the information and images posted online. Make considered decisions about posting any personal information regarding life experiences, experimentation, and relationships. Recognize that electronic mail (e-mail), in all forms, is not private and that the District reserves the right to access District provided e-mail as well as all other District data systems without notice or permission. If discovered, messages or data relating to, or in support of, illegal activities may be reported to the legal authorities.

2.2. **Protect Yourself.** Ensure that the information, images, and materials posted online will not put you at risk. Do not publish personally identifiable information such as addresses, phone numbers, birthdates, Social

Security numbers, contact details, personal schedule of activities, etc. Report any attacks or inappropriate behavior. Protect accounts, passwords, and resources, and change passwords in compliance with District policy. Never provide District login or password information over e-mail to anyone for any reason. Be aware that the District will never send an e-mail asking for information regarding any kind of security information such as a login name, password, etc.

2.3. **Respect Others.** Do not use electronic means to antagonize, bully, harass, or stalk others. Do not visit sites that are degrading, pornographic, racist, or otherwise inappropriate. Do not abuse rights of access, and do not enter other people's private spaces or areas. Be polite and do not become abusive in messages to others. Do not swear, or use vulgarities or any other inappropriate language. Do not use District systems or network in any way that would disrupt its use by others.

2.4. **Protect Others.** Report abuse and do not forward inappropriate materials or communications. Be aware of, and avoid, unacceptable materials and conversations. Do not reveal personally identifiable information (PII) of students or colleagues.

2.5. **Respect Intellectual Property**. Request permission to use resources. Cite any and all use of websites, books, and media. Acknowledge primary sources and validate information. Use and abide by fair use rules.

2.6. **Protect Intellectual Property**. Request permission to use software and media that others produce. Do not steal software and use only software that the District has purchased, licensed, and registered. Act with integrity and acknowledge that all communications and information accessible via District systems and network are private property.

3.0 Acceptable Use

3.1 Creation of files, projects, videos, web pages, podcasts, and other activities using electronic resources, consistent with the educational mission of the District and in compliance with district policy and procedure.

3.2 Participation in electronic communication and collaboration activities such as blogs, wikis, podcasts, email, and other activities using electronic resources, consistent with the educational mission of the District and in compliance with District policy and procedure.

3.3 Participation in district-sponsored social media to inform and communicate with members of the school district community consistent with the educational mission of the District and in compliance with District policy and procedure.

3.4 Use of electronic resources for incidental personal use in accordance with all District policies and guidelines.

3.5 Connection of any personal electronic device consistent with all guidelines in this document. Personal devices to be connected to the district main network must be approved by Information Technology Department.

3.6 Use of electronic resource accounts solely by the authorized owner of the account for the authorized purpose

4.0 Unacceptable Use

4.1 Unauthorized access or unauthorized disclosure of personal information of students, staff, or other individuals for whom the district retains records. "Personal information" includes education records, employment records, account and password information, and personal addresses, phone numbers, or email addresses.

4.2 Contributing to cyberbullying, chain letters, harassment, intimidation, denigrating comments, discriminatory remarks, and other similar conduct.

4.3 Using or forwarding profanity, obscenity, vulgar language, racist terms, or other language that is offensive to a reasonable person.

4.4 Any use of the electronic resources for individual profit or gain; for product advertisement; for political action or political activities; or for excessive personal use. “Political action or political activities” includes support of or opposition to political campaigns, candidates, ballot measures, or lobbying for or in opposition to legislation;

4.5 Intentionally seeking information on, obtaining copies of, or modifying files, other data, or passwords belonging to other users, or misrepresenting other users on the electronic resources.

4.6 Using an electronic account authorized for another person.

4.7 Making use of the electronic resources in a manner that serves to disrupt the use of the network by others.

4.8 Destroying, modifying, or abusing hardware and/or software.

4.9 Unauthorized downloading or installation of any software, including shareware and freeware, for use on Evergreen Public Schools electronic resources.

4.10 Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner other than use that falls within the scope of “reasonable fair use.” The “Fair Use Doctrine” of the United States Copyright Law (Title 17, USC) permits the duplication and/or distribution of materials for educational purposes under most circumstances.

4.11 Using electronic resources to access, process, or transmit obscene or pornographic content, sexually inappropriate content, or files dangerous to the integrity of the network.

4.12 Malicious use of the electronic resources to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system.

4.13 Any attempts to defeat or bypass the District’s Internet filter by using or trying to use proxies, https, special ports, modification to District browser settings or any other techniques, designed to avoid being blocked from inappropriate content or to conceal Internet activity.

4.14 Using any electronic resources for unlawful purposes.

4.15 Wasting District electronic resources, such as file space, printing or excessive bandwidth.

4.16 Modifying or changing system configurations without appropriate permissions.

4.17 Using District systems or network while access privileges are suspended or revoked.

5.0 Evergreen Public Schools Responsibilities

The question of Internet safety includes issues regarding the use of the Internet, Internet-ready, and other electronic devices in a manner that promotes safe online activity for children, protects children from cybercrimes, including crimes by online predators and cyberbullying, and helps parents shield their children from materials that are inappropriate for minors.

To promote the safe and appropriate online behavior of students as they access material from the Internet, the district will use the following four-part approach. However, given the ever-changing nature of the Internet, the district cannot guarantee that a student will never be able to access objectionable material. To these ends, the district reserves the right to, and may at any time, do the following:

- Log electronic resource use and monitor fileserver space utilization by users. The District assumes no responsibility or liability for files deleted due to violation of fileserver space allotments.
- Monitor the use of activities through the District's networks and electronic resources. This may include real-time monitoring of network activity and/or maintaining a log of Internet activity for later review.
- Provide internal and external controls as appropriate, including the right to determine who will have access to Evergreen Public Schools-owned equipment.
- Restrict or exclude those who do not abide by the Evergreen Public Schools' electronic resources policy or other policies governing the use of school facilities, equipment, and materials.
- Report to appropriate authorities apparent violations of the law discovered through the District's monitoring of electronic resources
- Restrict electronic resource destinations through software or other means.
- Provide guidelines and make reasonable efforts to train students in acceptable use and policies governing electronic resource communications.
- Monitor and maintain mailing list subscriptions and delete files from the personal mail directories to avoid excessive use of fileserver hard-disk space.
- Use filtering software to block or filter access to visual depictions that are obscene and all child pornography in accordance with CIPA. Other objectionable material may likewise be filtered. The determination of what constitutes "objectionable" material is determined by the District's administration consistent with the District's educational mission, the district's policies and procedures, and the board of directors' goals.

6.0 Legal Notices

No Expectations of Data Privacy:
The District reserves the right to access and disclose the contents of any account on any District system, including those hosted externally such as Gmail, without prior notice or permission from the account owner. As such, students have no expectation of confidentiality or privacy with respect to any communication or access made through District systems and network or on District-issued computers or mobile devices, regardless of whether that use is for District-related or personal purposes, other than as specifically provided by law. The District may, without prior notice or consent, log, supervise, access, monitor, view or record the use of District systems and network (including reviewing files and other materials) at any time. By using or accessing District technology, all students agree to such access, monitoring and/or recording of their use.

6.1 The Evergreen Public Schools is not responsible for the information that is retrieved via electronic resources.

6.2 Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq.), notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications. Network administrators have access to all email and will monitor messages.

6.3 Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

6.4 The District reserves the rights to monitor, inspect, copy, review, and store without prior notice any and all usage of:

- The network
- User files and disk space utilization (including cloud based solutions such as Google Drive and OneDrive).
- User applications and bandwidth utilization
- User document files, folders, and electronic communications
- Email
- Internet access
- Any and all information transmitted or received in connection with network and/or email use operated by or through District resources

6.5 All information files shall be and remain the property of the District, and no student user shall have any expectation of privacy regarding such materials. The District reserves the right to disclose any electronic message to law enforcement officials or third parties as deemed appropriate. All documents generated, received, transmitted, or maintained through district resources or networks are subject to the disclosure laws of the State of Washington's Public Records Act, chapter 42.56 RCW.

6.6 Backup is made of email for the purpose of public disclosure requests and disaster recovery. Barring power outage or intermittent technical issues tape backups are made of student files on District servers for recovery of accidental loss of deleted files. Recovery is not guaranteed.

6.7 While filtering software makes it more difficult for objectionable material to be received or accessed through district resources, filters are not infallible. The ability to access a site does not mean that otherwise objectionable material or an objectionable site falls within the district's acceptable use requirements. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites and/or materials. Any inadvertent visit to an objectionable site must be reported immediately.

6.8 From time to time, the Evergreen Public Schools will make determinations on whether specific uses of electronic resources are consistent with the Electronic Resources policy.

6.9 The Evergreen Public Schools will not be responsible for any damages users may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by our own negligence or user errors or omissions. Use of any information obtained is at the user's own risk.

6.10 The Evergreen Public Schools makes no warranties (expressed or implied) with respect to:

- The content of any advice or information received by a user or any costs or charges incurred as a result of seeking or accepting any information.
- Any costs, liability, or damages caused by the way the user chooses to use his or her access to the electronic resources.

6.11 The Evergreen Public Schools reserves the right to change its rules and procedures at any time without notification. 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.

- Age appropriate materials will be made available for use across grade levels.
- Training on online safety issues and materials implementation will be made available for administration, staff and families.

7.0 Personal Device Warning

7.1 By connecting a mobile device to the Evergreen Public Schools network, you acknowledge and agree that the Evergreen Public Schools Information Technology Department reserves the right to enforce any reasonable security measures deemed necessary to mitigate data leakage and protect students. This includes but is not limited to:

- Remotely deleting the contents of your mobile device when deemed necessary, e.g., when a password is incorrectly entered more than 10 times. The deletion may include district and personal contacts, pictures, etc.
- Enforcing the use of a password / pin to access the mobile device.
- Restricting the use of applications deemed a security risk.

7.2 In addition, users of district networks with personal devices understand that documents or records prepared, owned, used, or retained by any local or public agency – including the electronic communications of a public agency—are public records under Washington state law. Using any personal device or computer for school district business can result in a requirement that you submit your personal device for examination or search if a

public records request is received concerning information related to governmental conduct or the performance of any governmental function that may be stored on your personal device.

7.3 The mobile devices that are subject to this policy are those that directly connect to Microsoft Exchange/Office 365 via the ActiveSync Protocol.

7.4 Examples of ActiveSync compatible devices include but are not limited to: iPhone, iPad, iPod, Android based mobile phone, Tablet device, etc.

8.0 Violations of Acceptable Use

8.1 Any reasonable belief that user activity has violated this policy and procedure regarding acceptable use should be reported to the school, program, or department administrator responsible for supervision of the use in question. Disciplinary action, if any, for students and/or other users shall be consistent with the District's policies and procedures.

8.2 Violations of this policy can constitute reasonable cause for the limitation or revocation of access privileges, suspension of access to Evergreen Public Schools electronic resources. Violations may also result in school disciplinary action as well as other appropriate legal or criminal sanctions, as appropriate.

9.0 Challenging the Denial or Restriction of Access to District Electronic Resources

9.1 If a person is denied access or subject to restricted access to the District's electronic resources resulting from a determination that the person has violated the District's acceptable use standards, the denial or restriction may be appealed.

9.3 If access to electronic resources is denied or restricted for a student, the denial or restriction may be grieved consistent with the procedures for student discipline and as set forth in WAC 392-400-240. If access to electronic resources is denied or restricted for a student as part of a suspension or expulsion, the denial or restriction may be challenged consistent with the procedures and provisions of 3241P and chapter 392-400 WAC applicable to the suspension or expulsion imposed.

10.0 District-Provided Mobile Devices

Evergreen Public Schools students may be provided with a district owned mobile device for use at school and/or home. Technology ceases to be a scheduled event, freeing teacher and students to collaborate and create in real-time. The district's LIFT initiative is to create 21st learning environments that transforms the teaching and learning process for all students in the District to a more student-centered, teacher-facilitated experience that will lead to higher levels of engagement, empowerment and ultimately, academic achievement.

A mobile device can be defined as, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/tablet computers
- Ultra-mobile PCs (UMPC)
- Mobile/cellular phones
- Smartphones
- PDAs
- Any mobile device capable of storing corporate data and connecting to an unmanaged network

10.1 Security

All users of mobile devices must employ reasonable physical security measures. All users are expected to secure all such devices against being lost or stolen, whether or not they are actually in use and/or being carried. Mobile device must never be left in an unlocked locker, unlocked car or any unsupervised area.

In order to protect student Personally Identifiable Information (PII) and other confidential information, the mobile device will have a default to initiate a password-protected lock after 45 minutes of inactivity. User will not modify this to exceed the district 45 minute maximum. (PII consists of student names, addresses, contact information, email addresses, academic records/information, etc.)

Sharing a mobile device with another user can expose student Personally Identifiable Information (PII) and other confidential information to a party that should not have access to the data. Users should not share devices with family or friends.

In the event a mobile device is stolen or lost:

- Report the loss of the device immediately to your school administration and/or the district IT department so that it can be disabled to protect district information and initiate tracking of the device. (Computrace is software embedded in the programing of district mobile devices that are purchased as part of Evergreen LIFT initiative. In the event your mobile device is stolen, the Computrace software tracks the device and provides local police with the information they need to find it.)
- In the event theft is suspected, notify the Police of such theft and provide a copy of the police report to your principal or supervisor as evidence of the theft.

10.1.0 Connectivity to Unsecured Internet Access Points

With mobile devices, the potential exists to utilize unsecured Internet access points (airports, coffee shops, etc.). The use of such access may open up a mobile device to unauthorized users. Students will use discretion on the software applications accessed across unsecured networks.

10.2 Receiving Your Mobile Device and Check-In

10.2.0 Individually assigned equipment

All equipment will be tagged with an EPS asset tag, property sticker and endpoint security features such as Computrace. All mobile devices will be checked out and in through the district's inventory management system.

Mobile devices will be checked out to students at the beginning of the school year and will be returned during final week of school to the teacher librarian or the school designee, so it can be checked for serviceability.

An individual school's mobile device and accessories must be checked back in to the media specialist or other designee to be updated and serviced by the EPS IT Department at the end of each school year. Students who graduate early, withdraw, are suspended or expelled, or terminate enrollment in EPS for any other reason, or transfers within EPS must return their device on the date of termination or transfer. All accessories will need to be returned or a fee will be collected at that time.

10.2.1 Fees for missing or damaged Mobile Devices

If a student fails to return the mobile device, they are subject to financial liability until the device and its accessories are returned or associated fees are received. The student will pay the replacement cost of the device and all accessories. Failure to return the device within 5 working days after un-enrollment with EPS, may result in a theft report being filed with the appropriate local Police Department. Furthermore, the student will be responsible for repair or replacement costs due to any negligent damage to the device or accessories while under the student's care. Fees will not exceed the replacement cost for the items.

The EPS has already purchased a Device Coverage Program for all student mobile devices to lessen the financial burden if an accident or theft occurs. While the purchased program covers manufacturer defects, accidental damage, and theft, repair or replacement amounts may not always cover all associated costs. Therefore, while there is no user fee or damage deposit for the student device, Parents/guardians must be aware that they will be responsible for the following associated cost for damage, loss or theft.

Accidental Damage	Stolen	Negligent Damage	Not Covered
1st Incident $0 2nd Incident and beyond: $30 restock fee for each incident	1st Incident $0 2nd Incident and beyond: $30 restock fee for each incident	Damage: 1st Incident $30 deductible 2nd Incident and beyond $60 deductible & restock fee for each incident.	Lost devices (without police report) or intentional damage beyond repair: Device Age: Year 1 - $300 Year 2 - $200 Year 3 - $100
Covered: Accidental damage, fire, flood or natural disaster.	Police Report **is required** to file a claim.	i.e. Not using the provided case, exposing to weather,	Items to be replaced if needed at users expense. Cords Charger Case

- If the lost or stolen device is later recovered in working condition, the restock fee will be refunded.
- If a student leaves the District, but does not return the device, they will be fined for the full replacement cost, and standard rules for the restriction of records and transcripts would apply. Law enforcement may be involved for the purposes of recovering District property.

10.3 Taking Care of Your Mobile Device

Students are responsible for the general care of the equipment they have been issued by the district.

10.3.1 General Precautions

The Mobile Device is school district property and all users will follow these guidelines and the EPS acceptable use agreement for accessing and using electronic / digital resources.

- Only use a clean, soft cloth to clean the screen, no cleansers of any type.
- Cords and cables must be inserted carefully into the device to prevent damage.
- To minimize the possibility of damage, utilize the provided protective case (or utilize an equivalent protective case that you supply).
    - All users may personalize the protective case; however, any writing, drawing, stickers, or labels deemed inappropriate by EPS staff may not be used.
- Mobile device **must** remain free of any writing, drawing, stickers, or labels.
- Be sure hands are clean before using.
- Keep away from food and drink.
- Charge the device only with the included charger and using a standard wall outlet for your power source.
- Document any software/hardware issues as soon as possible, by notifying the IT Service Desk.
- Keep the device in a well-protected temperature controlled environment when not in use.

10.3.2 Screen Care

The device screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure on the screen.

- Do not lean on the top of the device when it is closed.
- Do not place anything on the mobile device that could put pressure on the screen.
- Do not place anything in a carrying case, brief case or back pack that could potentially break or cause damage to the device.
- Clean the screen with a soft, dry cloth or anti-static cloth.

10.3.3 Using Devices at School

Mobile device are intended for use at school each day. In addition to teacher expectations for device use, school messages, announcements, calendars and schedules may be accessed using the device. Students must be responsible to bring their device to all classes, unless specifically instructed not to do so by their teacher.

10.3.4 Mobile device Left at Home

If a student does not bring their device to school or class, they are responsible for getting the course work completed as if they had their device present. Repeat violations will result in action as detailed in the school's Parent/ Student Handbook Including Conduct and Discipline.

10.3.5 Undergoing Repair

Loaner Mobile device may be issued to students by the school when they leave their Mobile device for repair in the Media Center or other designated department if available. There may be a delay in getting a device should the school not have enough to loan. If a student's device is reported broken there may be a restock fee associated with the repair. It may be the responsibility of teacher or student/family to pay the fees, if applicable.

10.3.6 Charging Your Device / Battery

When students are allowed to take their Mobile device home the Mobile device must be brought to school each day fully charged. Students need to charge their Mobile device each evening.

10.3.7 Screensavers/Background photos

- Any media deemed inappropriate by EPS staff may not be used as a screensaver or background photo.
- Presence of guns, weapons, pornographic materials, inappropriate language, alcohol, drug, and gang related symbols or pictures are prohibited and will result in actions as detailed in the EPS Parent/Student Handbook concerning Conduct and Discipline.

10.3.8 Printing

Printing is discouraged due to collaborative and shared resources made available to students and staff. However, printing will be available through the teacher's computer. Students can work with teachers to print in instances where printing cannot be avoided. Printing at home will depend on the type of printer (district support not provided).

10.3.9 Home Internet Access

Students are allowed to connect to wireless networks on their Mobile device. The policies outlined in this document, EPS Acceptable Use Agreement and Procedures are applicable to home use of an EPS provided device. Any violation of the policy will result in the student's home use privilege being suspended.

If students experience Internet issues at home they should contact their Internet Service Provider (ISP) for support. While the device is off campus, it is the responsibility of the parents or guardians to monitor content searched and view by their student. EPS is not liable for content viewed by students while off school campus and after school hours. If a student does not have Internet access at home, information on affordable Internet plans are available by contacting the EPS IT Department.

10.4 Mobile Device Management (MDM)

Evergreen Public Schools uses mobile device management solutions to secure mobile devices and enforce policies remotely. The mobile device management solution enables IT to take the following actions on mobile devices: remote enterprise wipe, location tracking if needed to assist with theft or loss (default is disabled), corporate application visibility (no privately installed apps), and hardware feature management. Any attempt to contravene or bypass the mobile device management implementation will result in immediate disconnection from all District resources.

10.4 Software on Mobile Device

10.4.0 Inspection

Students may be selected at random to provide their device for inspection. If a student's device is requested for an inspection passwords to unlock device must be provided. EPS reserves the right to confiscate the device for any reason at any time if inappropriate materials are found on the device.

10.4.1 Procedure for re-imaging a device

If technical difficulties occur, illegal, or non-EPS installed software are discovered, the device will be restored from backup. The district does not accept responsibility for the loss of any software or documents deleted due to a restoration. If a device needs to be restored or software needs to be reloaded, a work order needs to be created with the IT Service Desk either by calling between 7:00 A.M and 4:00 P.M. or by using the web portal.

11.0 Connectivity

11.1 Network Connectivity

The Evergreen Public Schools will make every reasonable effort to ensure the network is reliable and secure. However, there is no guarantee the network will be up and running 100% of the time. In the rare case that the network is down, the District will not be responsible for lost or missing data.

It is a violation of the Acceptable Use Policies to use applications that bypass EPS Proxies and filtering. Repeat violations will result in disciplinary action as detailed in the EPS Parent/Student Handbook Including Conduct and Discipline.

Cross References:

Policy 2020	Curriculum Development and Adoption of Instructional Materials
Policy 2025	Copyright Compliance
Policy 3207	Harassment, Intimidation and Bullying
Policy 3231	Student Records
Model Policy 3241	Classroom Management, Corrective Actions or Punishment
Policy 4400	Election Activities

Legal Reference:

18 USC §§ 2510-2522	Electronic Communication Privacy Act
Pub. L. No. 110-385	Protecting Children in the 21st Century Act