# Guidelines for Responsible Use of Technology Resources (Staff)

Today
Futures to
Individual
Linking

Evergreen Public Schools

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.

While employees may have the occasion to communicate with students outside of the school day, the Evergreen Public Schools considers any electronic communication between an employee and a student to be an extension of the classroom or school. This extension immediately creates a nexus between the employee's job in the District and the portion of their private life involved in the communication. Employees should be aware that a parent or community member could easily misinterpret the various types of electronic communication between a staff member and an individual student. Therefore employees using e-mail, texting, twitter, Facebook or other means of electronic communication or social media with students must keep all communication professional, transparent, and appropriate. This includes word choices, tone, and subject matter that model the standards and integrity of a professional in the District. Employees are specifically prohibited from making sexual comments, sexual innuendos, compliments that focus on a student's physical attributes, from making sexist comments to students and from engaging in forms of discriminatory speech.

## 1.0 User Responsibilities

1.1 It is expected that staff and students will use electronic resources provided by the Evergreen Public Schools in work and study when using the district's internet and network. However, the failure of a staff member, 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.

1.3 District staff must at all times maintain the confidentiality of confidential student data in accordance with the Family Educational Rights and Privacy Act (FERPA) and corresponding state law.

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 administrative assistants, secretaries, managers, co-workers while on vacation, and family members. Do not write passwords down and store them anywhere in your office. 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 district staff members, log off of the device first. If a user is required to use your login information (such as a student teacher), you are responsible for their direct supervision. Remember: everything that happens on the network will happen under your username. Never share a logged in device with a student; staff members have elevated access to websites and district resources that are not always appropriate for student access. Never leave information systems containing personably identifiable and/or confidential information (PII) of student and/or staff logged in and unattended.

## 2.0 Public Records

2.1 Because the Evergreen Public Schools is a public agency under the Washington Public Records Act, chapter 42.56 RCW, any information or record relating to the conduct of government or the performance of any governmental functions that is prepared, owned, used, or retained by the district is a public record subject to disclosure upon request by any person. Such information may include retained records related to communications by or through district resources or records of Internet activity accessed by or through district resources. Whether such records, or any portion of such records, fall within the narrow exemptions of the Public Records Act will be determined once a request is received.

## 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 With parent permission, posting of student-created original educational material, curriculum-related materials, and student work. Sources outside the classroom or school must be appropriately cited and all copyright laws must be followed.

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

3.6 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.

3.7 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 Staff Responsibilities

5.1 Staff members who supervise students, control electronic equipment, or otherwise have occasion to observe student use of said equipment shall make reasonable efforts to monitor the use of this equipment to assure that it conforms to electronic resources procedures and is consistent with the mission and goals of the Evergreen Public Schools.

5.2 Staff should make reasonable efforts to become familiar with the electronic resources and their use so that effective monitoring, instruction, and assistance may be provided. Staff should report any misuse to their supervisor.

5.3 Outside of work hours, staff may use their district owned mobile device for personal use, given that this use does not violate the Unacceptable Use provisions in this document.

## 6.0 District-Sponsored Social Media (Teacher-Student Electronic Communication)

6.1 In the fast-changing world of electronic information and communication with parents, staff, and community members, the Evergreen Public Schools recognizes that social media tools can be of great value in furthering the district’s mission and promoting the board of directors’ goals. To those ends, approved schools and departments may be authorized to utilize social media in a manner consistent with state and federal law. The purpose of District-sponsored social media sites is limited to promoting the mission and goals of the district.

6.2 District staff will be authorized to access district-sponsored social media sites during work hours in support of the educational mission and goals of the district. District staff may only initiate a district-sponsored social media site for a school, department, class, activity, sport, or club when expressly authorized to do so by the Superintendent or the Superintendent's designee. All staff employees using district-sponsored social media sites will adhere to all of the acceptable use requirements as set forth. The inappropriate use of social media by district employees is a violation of this procedure.

6.3 District-sponsored social media sites are not intended to be used for policy decisions or items of legal and fiscal significance that have not been previously disclosed to the public. To avoid conflicts with Washington's Open Public Meetings Act, chapter 42.30 RCW, the board of directors will not engage in meetings or discussions via district-sponsored social media sites. Posting content via district-sponsored social media sites does not constitute giving official or lawful notice to the district as may be required.

6.4 The District may choose to allow user-generated content on its social media sites. By doing so, however, the District is not creating an open public forum. The purpose of such sites is to inform and engage with students and their families, staff, residents and other members of our community while promoting the mission of the district and the board of directors' goals. Although comments will not be removed based on viewpoint, comments and observations must be civil, constructive, respectful, and responsible. Because the district has a compelling interest in the lawful use of public resources and maintaining content that is appropriate for all users, the following content will not be permitted on social networking sites administered by the Evergreen Public Schools and is therefore subject to removal:

- Comments, posts or replies that are out of context and/or not related to the topic at issue.
- Comments in support of or opposition to political campaigns, candidates, ballot measures, or pending legislation.
- Sexual content or links to sexual content.
- Commercial advertisements or solicitations.
- Content that promotes, fosters, or perpetuates discrimination as prohibited by district policy.
- Language or content that is profane, vulgar, abusive, denigrating, harassing, intimidating, or bullying in nature.
- Conduct or encouragement of illegal activity.
- Content that tends to compromise the safety or security of the public or public systems, violate the privacy rights of individuals, or infringe on the legal ownership interests of any other party.
- Content that violates Evergreen Public Schools guidelines and procedures regarding the acceptable use of electronic resources.

6.5 Comments, observations, and other postings in violation of these guidelines will be removed by the District. Opinions expressed by third parties on District-sponsored sites are not those of the Evergreen Public Schools or its employees. Because the school district is a public agency, all comments posted on social networking sites administered by the district are public records that will be archived and subject to disclosure upon request.

6.6 District-sponsored sites will not be available for public comments or observations unless staff members have been designated to regularly monitor postings and verify compliance with District policy and procedure. EPS staff so designated will monitor public comment and observations on an established, regular schedule and will remove content in violation. All removed content will be archived as a public record.

6.7 Staff Guidelines for Social Media and Communication with Students:

- Work/Personal Distinction – Staff members must maintain a clear distinction between their personal social media use and any District-related social media sites.

- Limit On-Duty Use – Staff members must limit their personal technology use during duty hours. Use of personal technology should be limited to off-duty time and designated breaks.
- Student Photographs – Absent parent permission for the particular purpose, staff members may not send, share or post pictures, text messages, emails or other material that personally identifies students in electronic or any other form of personal technology. Staff members may not use student images, emails or other personally identifying student information.
- Professionalism – District employees must be mindful that any Internet content is ultimately accessible to the world. To avoid jeopardizing their professional effectiveness, employees are encouraged to familiarize themselves with privacy policies, settings and protections on any social networking websites to which they choose to subscribe and be aware that information posted online, despite privacy protections, is easily and often reported to administrators or exposed to District students.
- “Friending” District Students – Employees should not have online interactions with students on social networking sites outside of those forums dedicated to academic use. District employees’ social networking profiles and personal blogs should not be linked to District students’ online profiles.
- Contacting Students After School Hours – When in doubt about contacting a student outside of school hours using either District-owned or personal technology, begin by contacting the student’s parent(s) or legal guardian. Students should only be contacted for district/school-related purposes.

## 7.0 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 and staff 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 staff member 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 staff and 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.

## 8.0 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, staff 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 staff agree to such access, monitoring and/or recording of their use.

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

8.2 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.

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

8.4 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

8.5 All information files shall be and remain the property of the District, and no staff 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.

8.6 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 staff files on District servers for recovery of accidental loss of deleted files. Recovery is not guaranteed.

8.7 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.

8.8 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.

8.9 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.

8.10 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.

8.11 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.

## 9.0 Personal Device Warning

9.1 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.

9.2 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.

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

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

## 10.0 Violations of Acceptable Use

10.1 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 staff and/or other users shall be consistent with the District's policies and procedures.

10.2 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 employee discipline as well as other appropriate legal or criminal sanctions, as appropriate.

## 11.0 Challenging the Denial or Restriction of Access to District Electronic Resources

11.1 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.

11.2 If access to electronic resources is denied or restricted for an employee who is a member of a collective bargaining group because of a violation of the District's acceptable use standards, the denial or restriction may be grieved in accordance with the terms of the staff member's collective bargaining agreement. If the employee is not represented by a collective bargaining group, the denial or restriction may be appealed through the grievance process contained within the procedures for non-represented personnel.

## 12.0 District-Provided Mobile Devices

Evergreen Public Schools staff 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

### 12.1 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 principal, supervisor 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.

Identify to your principal or supervisor any PII or sensitive information that may exist on the device so the district can assess the potential degree of information breach.

#### 12.1.0 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. Staff will use discretion on the software applications accessed across unsecured networks. Staff should not have student personally identifiable information (PII) stored on a mobile device when using such networks as this could result in the PII being compromised.

### 12.2 Receiving Your Mobile Device and Check-In

#### 12.2.0 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 district staff when they take custody of the asset. District staff will retain the asset in their care and possession for as long as they are employed with the district or at which time the device needs to be replaced as part of the equipment refresh cycle.

Staff must check-in their mobile device either when their employment ceases with the district or when the employee is on an extended leave of absence. Staff may check in their device to their site teacher-librarian or other designee during extended breaks for secure storage.

#### 12.2.1 Student Mobile Device Carts

Carts of student mobile devices can be reserved and checked out through the local school Media Center or other designee. All equipment purchased as part of a cart will remain with the cart when stored. It is the responsibility of the reserving teacher to return equipment to the appropriate storage location with devices properly connected for charging, and to connect to power for recharging.

#### 12.2.3 Fees for missing or damaged Mobile Devices

If a staff member 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 staff member will pay the replacement cost of the device and all accessories. Failure to return the device within 5 working days after end of employment with EPS, may result in a theft report being filed with the appropriate local Police Department. Furthermore, the staff member will be responsible for repair or replacement costs due to any negligent damage to the device or accessories while under the staff member's care. Fees will not exceed the replacement cost for the items.

The District has already purchased a Device Coverage Program for all staff mobile devices to avoid any 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 fee or damage deposit for the mobile device, staff members 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<br>2nd Incident and beyond: $30 restock fee for each incident | 1st Incident $0<br>2nd Incident and beyond: $30 restock fee for each incident | Damage:<br>1st Incident $30 deductible<br>2nd Incident and beyond $60 deductible & restock fee for each incident. | Lost devices (without police report) or intentional damage beyond repair:<br>Device Age:<br>Year 1 - $1200<br>Year 2 - $900<br>Year 3 - $600<br>Year 4 - $300 |
| 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.<br>Cords<br>Charger<br>Case |
| • If the lost or stolen device is later recovered in working condition, the restock fee will be refunded.<br>• If a staff member leaves the District, but does not return the device, the replacement value of the device may be deducted from their final paycheck. | | | |

## 12.3 Taking Care of Your Mobile Device

Staff members are responsible for the general care of the equipment they have been issued by the district. Mobile device from the carts that are broken or fail to work properly must be reported for repair to the IT Service Desk.

### 12.3.1 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.

### 12.3.2 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.

## 12.4 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.

### 12.5 Software on Mobile 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.

## 13.0 Connectivity

### 13.1 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 4040 | Public Access to District Records |
| Policy 4400 | Election Activities |
| Model Policy 5281 | Disciplinary Action and Discharge |

Legal Reference:

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