Oak Ridge
SCHOOLS

Technology
Acceptable Use Policy &
Device Use Policy

Faculty and Staff

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

Acceptable Use Policy

Device Expectations

All Oak Ridge Schools employees, contractors, and volunteers must adhere to the district policies and procedures established by the Oak Ridge Schools Board of Education and the Human Resources Department.

Receiving a Technology Device: Technology equipment is assigned to individual staff members. To view technology items that are checked out to you, please visit the Destiny Library Catalog at library.ortn.edu, log in and select “My Info” at the top.

Computer Equipment Loan Agreement: Upon receiving an Oak Ridge Schools technology device, staff members will sign and return a Computer Equipment Loan Agreement (CELA) form.

Returning a Technology Device: Upon resignation or termination, all technology equipment must be returned to the Technology Department prior to the employee’s last day of employment.

Faculty and Staff Acceptable Use Guidelines

The purpose of the Oak Ridge Schools' district network is to support education, particularly in the areas of research and communications, by providing access to a multitude of electronic resources and opportunity to collaborate with other individuals and groups. Such open access is a privilege and requires that individual users act responsibly. Inappropriate or suspected inappropriate use could result in device confiscation, pending investigation. Violating federal or state laws or regulations or ORS policies or rules governing use of information technology may result in sanctions against the employee or contractor up to and possibly including immediate termination of employment or contract. Occurrences of inappropriate use will be determined by the Director of Technology and/or district administrators.

Each employee and contractor is responsible for lawful, Oak Ridge Schools (ORS)-compliant, ethical, and otherwise responsible use of ORS-provided information technology (IT) resources including computers, fax machines, district-issued cell phones and all other mediums of internet access. Users of ORS technology must be aware that ORS cannot assume any liability arising out of the illegal or inappropriate use of technology resources.

Inappropriate conduct carried out on the previously listed electronic systems includes, but is not limited to, the following:

- Revealing others' personal information, such as an address or phone number, without auditable record of authorization;
- Making unauthorized copies of ORS files or data;
- Destroying, deleting, erasing, or concealing ORS files or other data, or otherwise making such files or data unavailable or inaccessible to ORS or other authorized users;
- Violating student privacy by sharing personal information that goes against Personal Identifying Information (PII) rules and regulations;
- Participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate ORS purposes;
- Engaging in excessive use of instant messaging and chat rooms for personal purposes unrelated to one's position with ORS;
- Accessing networks, servers, drives, folders, files, or accounts to which the employee has not been granted access;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Sending, receiving, or accessing pornographic materials;
- Becoming involved in partisan politics or running for office;
- Soliciting or selling products or services unrelated to ORS;
- Causing congestion, disruption, disablement, alteration, or impairment of ORS networks or systems;
- Taking part in electronic gambling activities;
- Accessing personal social media sites on school computers or during school hours except for instructional purposes;
- Utilizing images, videos, written word or other such media that falls under copyright. Exceptions are made when duplication or distribution of materials for educational purposes is permitted when such duplication or distribution would fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC);
- Destroying, modifying or abusing any ORS IT hardware or software, including circumventing internet content filters or network safety measures;
- Installing any unauthorized software, including shareware and freeware, for use on ORS district's network;
- Misrepresenting oneself or ORS;
- Engaging in unlawful or malicious activities;
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the ORS networks/systems or any network/system;
- Taking part in any activity that serves to disrupt the use of technology by other users;
- Defeating or attempting to defeat security restrictions on ORS systems and applications;

Using ORS electronic systems to access, create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material, defined as any visual, textual, or auditory entity, file, or data, is strictly prohibited. Such material violates ORS anti-harassment policies and subjects the employee responsible to disciplinary action. ORS's e-mail system, Internet access, and computer systems must not be used to harm others or to violate the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way. Use of ORS resources for illegal activity can lead to disciplinary action, up to and including dismissal and/or criminal prosecution.

Each employee, contractor, sponsored account or other Net ID holder shall acknowledge having read and will pledge to adhere to the terms, spirit, and intent of this agreement as well as to report any known instances of violations of the agreement by others before being given access to ORS information technology resources.

Privacy

To maintain network integrity and ensure the network is being used responsibly, local school Instructional Technology Coaches, Technicians, and/or other designated staff reserve the right to inspect any and all data, including data stored by individual users on individual school or personal devices (if connected to the ORS network).

ORS owns the rights to all data and files in any computer, network, or other information system used within the district and to all data and files sent or received using any system or using ORS access to any computer network. These rights are not superseded by applicable laws related to intellectual property. These rights apply to electronic data belonging to both current and past ORS employees. Any intellectual property created during working hours or through the use of ORS devices and/or programs is the property of ORS.

ORS reserves the right to monitor e-mail messages (including personal/private/instant messaging systems) and their content, as well as any employee use of the Internet and of computer equipment used to create, view, or access e-mail and Internet content. Any e-mail messages sent and received using ORS equipment or ORS Internet access are not private and are subject to viewing, downloading, inspection, release, and archiving by ORS at any time. ORS has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to assure compliance with ORS policies as well as state and federal laws. ORS has the right to gather electronics for disposal or investigation.

Accordingly, employees should assume that whatever they do, type, enter, send, receive, and view on ORS electronic information systems is electronically stored and subject to inspection, monitoring, evaluation, and ORS use at any time and without notice. Because of this, users are encouraged to avoid storing personal and/or private information on technology devices or network resources owned by ORS.

Data Security

Staff members are expected to follow all local, state, and federal laws in addition to this Acceptable Use Policy and Internet Safety Agreement regarding the protection of student and staff confidential data.

Individuals may not attempt to log into the network using any account and/or password other than the login(s) assigned to them. Hacking or attempting unauthorized access to any computer are prohibited as is trespassing in another's folders, work or files.

District or school data, such as but not limited to Skyward student information, accessed through school system technology resources may not be used for any private business activity.

All unattended computing equipment should be password protected (e.g., screen locked, logged off, etc.). Students should NOT be allowed access to a teacher/administrator/staff's computer.

The employee understands that any data (documents, passwords, email, or other form) obtained during the performance of work duties must remain confidential. ORS data should NEVER be stored on personal data storage devices unless an employee is acting as an independent contractor for the district; in this case, all data pertaining to Oak Ridge Schools must be permanently and immediately removed from any personally owned data storage devices upon leaving Oak Ridge Schools' employment. Any hardcopies of data (documents, passwords, email, or other form) must be submitted to your immediate supervisor or destroyed upon exiting employment. The employee understands that possession of data after the termination of employment that results in any breach of confidentiality is grounds for disciplinary action and possible liability in any legal action arising from such a breach.

The system-wide technology staff performs routine backups in an effort to assure continuity of business. There can be no assurance, however, that technology resources will be available within a particular time frame following an outage. There is no guarantee that information that existed prior to an outage, malfunction, or deletion can be recovered. Users are expected to maintain and back up critical files and data.

Student Data Non-Disclosure

Staff members are prohibited from disclosing any private student information outside the school system or storing/saving this information on external storage devices. This information includes, but is not limited to, data containing social security numbers, information protected by the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), Protection of Pupil Rights Amendment (PPRA), and any other sensitive and/or protected information.

In addition, any information (written, verbal, electronic, or other form) obtained during the performance of one's duties must remain confidential. This includes all information about students, families, employees, associate organizations, or tests as well as any other information otherwise marked or known to be confidential. Staff members should avoid rostering or transmitting student data within unauthorized applications.

If you have any questions about student data or specific circumstances, please reach out to the Director of Technology for clarification.

Email

ORS provides access to email accounts for all employees. All messages within the email system are the property of Oak Ridge Schools. Personal use of email is permitted as long as it is limited and does not violate this policy, adversely affect others, interfere with the performance of any job responsibilities, or adversely affect the speed of the network.

If you receive an email that violates the guidelines below, please inform your supervisor.

General Guidelines

Any emails pertaining to ORS business that are composed or read on personally owned computers are not considered confidential. Please see the board of education's policy concerning the use of email. [Board Policy 1.805]

General guidelines for using an ORS email account are listed below:

- Any communication that is obscene, racist, sexist, pornographic, vulgar, threatening, harassing, disruptive, intentionally disrespectful, or otherwise prohibited by law is strictly prohibited.
- Do not use access to make, distribute, or redistribute jokes, stories, or other material based on slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.
- ORS email accounts may not be used for political activity, personal gain, commercial purposes, or profit.
- ORS email accounts may not be used for attempting to send anonymous messages. ORS email accounts may not be used for sending mass emails except for Oak Ridge School's educational purposes. When sending mass emails for educational purposes (including as a Reply All email or to a whole school), please seek permission from your supervisor before sending.
- When sending messages to multiple parents and families at the same time through Skyward message center, please limit your attachment size so that the communication is not delayed.
- Be considerate when sending email attachments. Be sure the file is not too large to be accommodated by the recipient's system and is in a format the recipient can open. If the attachment must be sent to a large number of recipients, be mindful that the network may be burdened by the size of the attachment multiplied by the number of recipients, thus inducing delayed transmission and receipt.
- Users should regularly delete electronic messages and any unnecessary files to limit storage space being utilized by their account.
- ORS email accounts may not be used for posting or forwarding another user's personal communication without the author's consent. This expectation does not apply to professional communications, which may be forwarded.
- Because email is not securely transmitted, discretion must be used when sending or encouraging the receipt of email containing sensitive information about students, families, school system employees, or any individuals. There can be no assurance that email will be confidential and/or private.
- It is not permitted to send personal, identifiable information about staff, students or families outside of the ORS email system without password protection/encryption. Personal, identifiable information includes any of the following: full name with birthday, student work samples with name attached, social security numbers, test data with names attached, medical information, etc.
- Even when password-protecting/encrypting the information, be careful that the person to whom the information is sent has permission to have this information. Under FERPA, schools may not disclose personally identifiable information from a student's education records to a third party unless written consent has been provided (with a few exceptions). When password-protecting/encrypting the document, send the password to the intended recipient using a different communication channel. See instructions for proper email encryption located in our Tech Tips portal at www.ortn.edu/technology.
- Do not assume that a sender of email is giving permission to forward or redistribute the message to others or to divulge the sender's email address to third parties. This should only be done with the sender's permission.
- Always delete email or other messages from unknown or untrustworthy senders, suspicious files, links, or URLs. These can contain malicious software or viruses.
- Use a signature on the bottom of your email in which you identify your name, phone number, job title, and location

Please remember that email communication can be accessed as part of the Tennessee Public Records Act. Please consider each communication as something that could potentially be viewed by the public and write it accordingly. There is no expectation of privacy.

Email Retention

All emails sent to or from ORS email accounts will be retained indefinitely until the email is deleted by the user. Once the email is deleted, it will be retained for a period of three (3) years. Exceptions to this rule include the following:

- Saved emails belonging to an employee email account will begin the retention period on the day of said employee's final day of employment with ORS.

- Any emails deleted over the course of an employee's employment period with ORS will begin the retention period on the date of the messages' deletion.
- Any ORS email account placed on litigation hold will be retained indefinitely or until litigation hold is removed from the account.

Security

Incoming and outgoing email is filtered by the district for inappropriate content. However, no filtering system is foolproof, and material deemed inappropriate by individual users may be transmitted despite filtering. ORS cannot assume any liability for such breaches of the filter.

Use a secure password for your email account and take note of the following guidelines:

- Do not use dictionary words, names or dates.
- Use a mixture of alphabetic, numeric and special characters.
- Have a minimum length of eight characters.
- Do not publicly display your password.
- Do not share your password.
- Log off and and/or lock your computer when leaving it unattended.
- Regularly change your password.

At the discretion of the Superintendent or designee, email accounts may be locked without notice.

Internet Use

The intent of ORS is to provide access to resources available via the internet with the understanding that staff and students will access and use information that is appropriate for their various curricula. All school rules and guidelines for appropriate technology usage, as well as local, state, and federal laws, apply to usage of the internet. Educators should always screen all internet resources prior to use with students.

Internet activity can and will be monitored, along with other aspects of technology usage. Internet access for all users is filtered through one central point by Uniform Resource Locator (URL) (web address) and by Internet Protocol (IP) address and may be filtered by keyword. URLs and IP addresses may be added to or deleted from the filtered list by the Director of Technology and his/her designee. Staff members may request to review filtered categories. Users requesting sites for blocking or unblocking must list specific URLs.

All ORS policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, district information dissemination, standards of conduct, misuse of resources, anti-harassment, and information and data security.

Successful or unsuccessful attempts to bypass the internet filter by using proxies or other resources are a violation of this agreement.

Creation of Web-Accessible Materials

ORS users with access to blogs, wikis, podcasts, Google applications, and social networking sites, are required to keep personal information out of their postings. The website is limited to usage associated with activities of ORS. The website or other online publishing applications cannot be used for personal financial gain, to express personal or political opinions, or to editorialize. The Technology and Communications staff reserves the right to reject all or part of proposed or posted content.

Student pictures or other personally identifiable information may be used in accordance with the consent of the student's parent/guardian and in accordance with the Children's Internet Protection Act (CIPA) and FERPA guidelines. Personal, identifiable information examples include home and/or school address, work address, class and/or school phone numbers, full name, social security number, etc.; no personal, identifiable information shall be published on or linked to on the website.

Caution should be used when photographs of any students are included on webpages. Group photographs without names are preferred for all students. No last name of other personal demographic information will appear with any student likeness except for recognition for honors or awards with parent/guardian consent.

Social Media

Social media can be a valuable tool for both personal and professional use. Employees who manage officially recognized social media accounts are expected to post important, relevant, and interesting material. Employees should strive to only post information that will be useful to and appreciated by the community/network. ORS approved users of social media are expected to maintain social media accounts/fan pages and are expected to post at least two to three times per week to keep accounts current and relevant. ORS approved users of social media are expected to refrain from allowing personal or political viewpoints to dictate the kind of information they share. Approved users are always expected to carry themselves professionally and represent ORS positively.

Please note that any “liking”, “linking”, “retweeting”, or subscribing to another post or “fan page” does not constitute an endorsement on the part of ORS of that post, page, creator or his/her opinion, product, or service. The same applies to comments posted by others to ORS social media accounts.

The guidelines below have been developed to help protect students and employees from charges of inappropriate use. Although many of the items below specifically reference Facebook and Twitter, the guidelines and cautions apply to all social networking sites.

ORS must approve all ORS professional social media accounts bearing an ORS logo and the account users must adhere to the following:

- Approved naming convention for all social media accounts as determined by the Director of Technology.
- All information and posts must be archived on the particular social media site or according to archiving procedures as determined by the Director of Technology or Communication Supervisor.
- All social media accounts must use ORS domain accounts as their setup accounts and an approved password recovery account provided by the Director of Technology.
- Passwords need to be changed every six months and should follow these guidelines:
    - Is at least eight characters long (if permitted by the site)
    - Does not contain your username, real name, or company name
    - Does not contain a complete word
    - Is significantly different from previous passwords
    - Contains characters from each of the following four categories:
        - “UPPERCASE” LETTERS
        - “lower case” letters
        - Numbers (1, 2, 3, 4, etc.)
        - Symbols found on the keyboard (all keyboard characters not defined as letters or numerals) and spaces

A professional social media account is encouraged to be set up instead of “friending” or “following” personal accounts*.* It is strongly recommended that teachers do not “friend” or “follow” current students and/or students under 18 years of age.

District sponsored sites such as Canvas and Skyward parent portals should be the primary means for electronic parent/student communication. Personal messaging to a student is discouraged and all communications should be carried out on the listed sites’ public messaging/comment areas.

District staff are prohibited from accessing personal social networking sites on school computers or during school hours except for legitimate instructional purposes.

ORS has created and hosts options for teachers to safely use social media for instructional purposes. As part of these offerings, ORS has designated a Communication Supervisor to provide guidelines for staff members to aid them in responsible use of social media for the protection of ORS students and staff.

ORS reserves the right to monitor and conduct random “spot checks” by the Communication Supervisor, Technology staff or administrators to ensure compliance with the guidelines provided. ORS reserves the right to delete comments that use foul language, links to unacceptable web sites, or anything that is in any way abusive to employees or other followers. ORS reserves the right to block subscribers who are abusive to employees or other followers. Do not respond to inflammatory or inappropriate messages by any means.

Copyright

Any questions about copyright provisions should be directed to the Director of Technology.

Legal and ethical practices of appropriate use of technology resources as well as digital citizenship will be taught to students and employees in the system. Again, all questions regarding legal and ethical practices of appropriate use should be directed to the local school Instructional Technology Coach and/or district Director of Technology.

Copyright is implied for all information (text, data, and graphics) published on the internet. Employee webpage authors will be held responsible for the content of their pages. Do not "borrow" icons, sounds, or graphics from other pages without documented permission. It is the employee's responsibility to secure proper usage permission. When possible, electronically link to information rather than duplicating online or printing for student use. Duplication of any copyrighted software is prohibited unless specifically allowed in the license agreement and should then occur only under the supervision and direction of the Technology staff.

Device Use Policy

Technology Device Use Overview

Faculty and staff are responsible for using the technology device according to school and district policies, and the care of the technology device is the employee's responsibility. Employees should not lend their device to another employee or individual. Each technology device is assigned to an individual staff member and the responsibility and care of that device rests solely with that staff member.

Technology Device Guidelines

Care and Maintenance

- Use a backpack, laptop case or other bag to carry technology equipment. Consider carrying the device in a bag with a designated laptop sleeve for further protection. Always make sure the laptop is placed in a bag with the port side facing up.
- Devices should never be picked up by the lid. Close the device before picking it up.
- Technology equipment should be kept at room temperature and not exposed to extreme temperatures.
- Do not leave technology equipment in a vehicle or outside.
- Liquids and food should not be used/consumed in the vicinity of the technology equipment.
- Faculty and staff should not write on, draw on, or add stickers to any equipment.
- The device should never be placed in an area where it could accidentally be sat or stepped on. In addition, devices can be a tripping hazard when charging.

Cleaning Technology Equipment

- Cleaners, sprays, alcohol, ammonia or abrasives should not be used on the technology equipment.
- Technology equipment should be cleaned with a soft, lint-free cloth.

Maximizing Battery Life

Staff should use the technology device in ways that maximize its battery life. See our tech tip at https://www.ortn.edu/district/technology/help/tech-tips/ for a step-by-step.

- ***Battery Saver:*** The Energy Saver control panel offers several settings that can adjust power levels for the device. Adjusting these settings will allow the device to dim the screen and use other components sparingly when it is not plugged in to charge. This helps preserve battery.
- ***Brightness:*** Students should dim the screen to the lowest comfortable level to achieve maximum battery life.
- ***Bluetooth Wireless:*** You may also turn off Bluetooth to maximize battery.
- ***Applications and Peripherals:*** Disconnect peripherals (external devices like headphones or keyboards) and completely quit and close applications that are not in use.

Repair and Replacement Guidelines

The following is designed to be a guide and reference for dealing with issues related to staff technology device damage with the understanding that the goal is for every employee to have an operational device. Typically, issues will arise over one of the following: Theft, Loss, Non-preventable Damage, Unintentional Damage/Negligence, and Intentional (Malicious) Damage/Recklessness.

Theft/Loss/Non-Preventable Damage

For Theft:

- The theft must be reported as soon as possible and no longer than 5 days after the incident.
- A police report is required to document the theft of a technology device.
- Upon finalizing the report, the staff member will be issued a new computer.
- Please see the damage matrix below for damage penalties related to stolen devices.

For Loss:

- The lost device must be reported immediately to school administration no longer than 5 days after the loss. Once damage penalties are received, a new device will be issued.
- For damage penalties related to lost devices, please see the damage matrix below.

For Non-Preventable Damage:

- These cases are rare, but examples include, but are not limited to an auto accident or a house fire.
- Upon determination of a verifiable accident, the staff member will be issued another device.

Unintentional Damage/Negligence

Damage must be reported as soon as possible within a window of 5 days from the time of the damage unless the damage occurs during a break; in this case, the damage must be reported within 5 days of the staff member's return to school. This includes any mobile technology device or CELA receipt device issued to the employee.

Employees have accepted responsibility for the technology device and therefore are liable for the cost of the repair or full replacement cost of the device. The first three instances of unintentional damage within a school year will be repaired free of charge; however, penalty fees will be received for a fourth incident of unintentional damage and subsequently for each additional incident within a school year.

- For damage penalties related to unintentional damage, please see the damage matrix below.
- The replacement cost of the device cannot be satisfied by employees purchasing their own replacement device from a third party.

Intentional (Malicious) Damage/Recklessness

Damage must be reported as soon as possible within a window of 5 days from the time of the damage unless the damage occurs during a break; in this case, the damage must be reported within 5 days of the staff member's return to school. This includes any mobile technology device or CELA receipt device issued to the employee.

Employees have accepted responsibility for the technology device and therefore are liable for the cost of the repair or full replacement cost of the device in an instance of intentional (malicious) damage.

- The cost of repairs will be assessed for each reported incident.
- The replacement cost cannot be satisfied by employees purchasing their own replacement equipment/device from a third party.
- Please note that intentional damage also includes damage to asset tags. It is not acceptable for any employee/contractor to intentionally remove asset tags and other device identifiers.
- The determination between accidental and intentional/malicious damage will be made by building administration or the employee's direct supervisor.

Accessories Damage and Replacement

Damage to laptop accessories such as styluses or chargers will be repaired when possible. If repair is not possible, or if accessories have been lost/stolen, the staff member will be responsible for purchasing a replacement directly from the Technology Department. Replacement accessories may not be purchased from a third party.

Please see the matrix below for costs associated with replacement technology accessories.

Penalty Damage Matrix

The following tables summarize the consequences of the various damage scenarios for the technology device, including the device itself, charger, and any other accessories.

The maximum out-of-pocket cost for damages will not exceed $50 per act of unintentional damage. Other penalties may be added on a case-by-case basis.

Machines and associated repair costs are divided into two categories: production and non-production.

Production machines are those that, if broken, will be repaired and given back to the employee. These machines are considered more “high-end” and therefore have a higher repair cost. Production machines include, but are not limited to, the following model types:

- Lenovo Yoga L13
- Lenovo Yoga 380
- Lenovo Yoga 390
- Lenovo Yoga X13

Non-Production machines are those that, if broken, will be replaced with a production machine because the district no longer services them. Non-production machines include, but are not limited to, the following model types:

- Lenovo Yoga 260
- Lenovo Yoga 220
- Lenovo Yoga 12

Production Machines	
Damage	**Financial Consequence**
School-Issued Laptops and Accessories	
Wear and Tear	No penalty
Charger Damage/Replacement Needed	$17 replacement cost
MiFi Device	$35 replacement cost
iPad Device	$50 penalty up to full replacement cost
Laptop Stylus	$30 replacement cost
Unintentional Damage for a 1st, 2nd, or 3rd offense in a year (includes more than one incident within the school year)	No penalty
Unintentional Damage for 4 or more offenses	$50 penalty
Stolen Device	$50 penalty/replacement cost
Lost Device	Up to full replacement cost
Intentional (Malicious) Damage	Full replacement cost
School-Issued Cell Phones	
Smartphone	Up to full replacement cost depending on device age and damage type
Flip Phone	N/A

Non-Production Machines	
Damage	**Financial Consequence**
School-Issued Laptops and Accessories	
Wear and Tear	No penalty
Charger Damage/Replacement Needed	$17 replacement cost
iPad Device	$50 penalty up to full replacement cost
Laptop Stylus	$30 replacement cost
Unintentional Damage for a 1st, 2nd, or 3rd offense in a year (includes more than one incident within the school year)	No penalty
Unintentional Damage for 4 or more offenses	$50 penalty
Stolen Device	$50 penalty/replacement cost
Lost Device	Up to full replacement cost
Intentional (Malicious) Damage	Full replacement cost

If an employee’s work phone bill is high due to excessive use of 411 or other programs, the employee will be responsible for paying such charges.

Applicable Laws

FERPA: www2.ed.gov/ferpa

CIPA: http://www.fcc.gov/guides/childrens-internet-protection-act
COPPA: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0
PPRA: https://studentprivacy.ed.gov/faq/what-protection-pupil-rights-amendment-ppra

Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq.), notice is hereby given that no facilities are provided by ORS for sending or receiving private or confidential electronic communications. Network administrators have access to all email and monitor messages. Messages in the generation or furtherance of illegal activities will be

Employee Name ______________________________________

Employee Signature___________________________________ Date__________________