Oak Ridge Schools

Office of the Superintendent

Administrative Procedure 1.805, 4.406, 4.407
Acceptable Use of Technology Device, Email, Internet & Website

Table of Contents

Device Expectations 3
- Technology Device Use 3
- Technology Device Guidelines 3

Repair and Replacement Guidelines 4
- Theft/Non-Preventable Damage 4
- Accidental Damage/Negligence 4
- Willful Damage/Recklessness 4

Non-Student Acceptable Use Guidelines 5
- Access 5
- Privacy 6
- Data Security 6
- Student Data Non-Disclosure 7
- Copyright 7
- Email 8
  - *General Guidelines* 8
  - *Security* 9
- Internet Use 9
- Web Publishing 9
- Social Media 10
- Netiquette 12
- Information Technology Acceptable Use 12
- Information Technology Unacceptable Use 13
- Applicable Laws 14

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 Resource 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.

Computer Equipment Loan Agreement: Upon receiving an Oak Ridge Schools technology device, staff members will sign 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.

Technology Device Use

- Faculty and staff should not write on, draw on, or add stickers to any equipment.
- Faculty and staff are responsible for using the technology device according to school and district policies.
- 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

- It is recommended that faculty and staff use a backpack, laptop case or other bag to carry their technology equipment.
- Devices should never be picked up by the lid. Faculty and staff should close the Technology Device before it is picked up.
- Technology Equipment should be kept at room temperature and should not be exposed to extreme temperatures.
- Faculty and staff should not leave their Technology Equipment in a vehicle or outside.
- Liquids and food should not be used/consumed in the vicinity of the Technology Equipment.
- The Technology Equipment should not be in a place where someone could accidentally sit or step on the equipment.
- Devices can be tripping hazards when they are charging. Please be very careful to charge your device in such a manner that others will not trip over the wire.

Cleaning the 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.

Maximize Battery Life

Faculty and staff should use technology equipment in a way that maximizes its battery life.

- **Energy**: The energy saver control panel offers several settings that determine power levels for the technology device. The technology device knows when it is plugged in, and runs accordingly. When on battery power, it will dim the screen and use other components sparingly. If you change this setting to maximize performance, your battery will drain more quickly.

- **Brightness:** Dim the screen to the lowest comfortable level to achieve maximum battery life. For instance, when watching a video in a dark room, you may not need full brightness.
- **AirPort Wireless:** AirPort consumes power, even if you are not using its features to connect to a network. You can turn it off in the control panel to save power.
- **Bluetooth Wireless:** Likewise, you can turn off Bluetooth to maximize your battery life, as it also consumes power when not in use.
- **Applications and peripherals:** Disconnect peripherals and quit applications not in use.

Repair and Replacement Guidelines

The following is designed to be a guide and reference for dealing with issues related to non-student 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, Non-preventable Damage, Preventable Damage/Negligence, and Willful Damage/Recklessness.

Theft/Non-Preventable Damage

- **For Theft:**
  - The theft must be reported as soon as possible.
  - A police report is required to document a theft.
  - Upon finalizing the report, the staff member will be issued a new computer.
- **For Non-Preventable Damage**
  - These cases are rare, but examples might 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 computer.

Accidental Damage/Negligence

Damage must be reported as soon as possible within a window of one week from the time of the damage unless the damage occurs during a break; in this case, the damage must be reported within one week of the staff members 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 repair and/or replacement of the device will be free of charge for accidental damage or negligence during the lifetime of the device. After the first free repair and/or replacement, the following penalty guidelines will apply:

- If the computer is damaged but repairable, a penalty fee for up to $50 will be assessed.
- The replacement cost of the device cannot be satisfied by employees purchasing their own replacement.

Willful Damage/Recklessness

Damage must be reported as soon as possible within a window of one week from the time of the damage unless the damage occurs during a break; in this case, the damage must be reported within one week of the staff members 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 cost of repairs will be assessed for each reported incident.
- The replacement cost cannot be satisfied by employees themselves purchasing their own replacement equipment.
- Please note that willful damage also includes asset tags. It is not acceptable for any employee/contractor to intentionally remove asset tags and identifiers.
- The determination between accidental and willful damage/recklessness will be made by the property recovery committee.

Non-Student Acceptable Use Guidelines

The purpose of the Oak Ridge Schools' Education Network (ORSEN) 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. Computers and networks provide access to local resources, as well as the ability for worldwide communications. Such open access is a privilege and requires that individual users act responsibly.

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. 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, including dismissal from employment or service.

Users must respect the rights of others and the integrity of the computer network and observe all relevant laws and regulations. All users are subject to existing laws (federal and state) and ORSEN policies, including not only those laws and regulations specific to computers and networks but also those that apply generally to personal conduct. Users are expected at all times to base their actions on rules of common courtesy and respect for others.

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

Each user's signed agreement will be kept on file. Each user may be required to sign an updated agreement at any time and without prior notice at the discretion of the Superintendent or designee.

Access

The use of all ORS technology resources is a privilege, not a right, and inappropriate or suspected inappropriate use can result in a cancellation of those privileges, pending investigation. Moreover, users of ORS technology must be aware that ORS cannot assume any liability arising out of the illegal or inappropriate use of technology resources. The Director of Technology, local school Instructional Technology Coaches, the Communications Supervisor and/or school system administrators will determine when inappropriate use has occurred, and they have the right to deny, revoke, or suspend specific user accounts.

- Individuals may use only accounts, files, software, and/or other technology resources that are assigned to, provided, or approved for him/her.
- Individuals identified as a real or suspected security risk can be denied access.
- Any use of technology resources that reduces the efficiency of use for others can be considered a violation of this agreement.
- Personal technology-related devices (if connected to the ORS network), such as but not limited to laptops, mobile devices, smartphones, and tablets, used on school grounds are subject to all items covered in this agreement and other applicable published guidelines.

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). Users should be aware that activities are subject to being monitored at any time and without notice.
- Users should not have any expectation that their use of technology resources, including files stored by them on the ORS network, will be private and will be secure from access by others. Reasonable steps will be taken to maintain the security of technology resources, but no assurance can be given that penetration of such security will not occur. Because communications on the internet are public in nature, all users should be careful to maintain appropriate and responsible communications. ORS cannot guarantee the privacy, security, or confidentiality of any information sent or received via the internet.
- 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 network account and/or password other than the login(s) assigned to him/her. Individuals may not allow someone to use his/her network account and/or password to access the network, email, or internet. 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.
- The employee understands that any data (documents, passwords, email, or other form) obtained during the performance of my duties must remain confidential. Therefore, all data pertaining to the Oak Ridge Schools must be permanently and immediately removed from any personal 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.
- Additional, all Oak Ridge Schools-owned equipment (computers, phones, keys, etc.) must be immediately turned in to your supervisor upon exiting employment with Oak Ridge Schools.

- 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 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 or personal portable devices that do not remain on campus. This information includes, but is not limited to, data containing social security numbers, information protected by Family Educational Rights and Privacy Act (FERPA), and any other sensitive and/or protected information. In the event that this type of information is stored on a portable or external device and said device is lost or stolen, the Director of Technology should be notified immediately.
- Any questions about student data or specific circumstances shall be directed to the Director of Technology for clarification. Violations of the use of student data or information will be handled in a manner consistent with comparable situations requiring disciplinary and/or legal action.
- In emergency situations, student pictures or other personally identifiable information may be shared with outside agencies in accordance with Family Educational Rights and Privacy Act (FERPA) guidelines.
- Any information (written, verbal, electronic, or other form) obtained during the performance of ones 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. Any unauthorized release or carelessness in the handling of confidential information is considered a breach of the duty to maintain confidentiality. Any breach to maintain confidentiality is ground for disciplinary action (up to and including immediate dismissal) and possible liability in any legal action arising from such breach.

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.

Email

ORS provides access to email accounts for all employees. Technical support is provided for ORS email accounts used to conduct educational and/or instructional business. 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

- In the course of conducting Oak Ridge Schools' business, an employee of Oak Ridge Schools must use their Oak Ridge Schools' email account. It is prohibited to conduct official business while using one's personal email address.
- Any communication that is obscene, racist, sexist, pornographic, vulgar, threatening, harassing, disruptive, intentionally disrespectful, or otherwise prohibited by law is strictly prohibited.
- 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 educational purposes. When sending mass emails for educational purposes (including as a *Reply All* email or to a whole school), please get permission from your supervisor before sending it out.
- 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 personally identifiable information about staff, students or families outside of the ORS email system without password protection/encryption. Personally identifiable information includes 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.
    - Verify that this information is transmitted only to the intended recipient by verifying the recipient's address and ensuring it is not contained in a "reply all" email.
- There is a system-imposed limit on storage for email accounts. Users meeting or exceeding the limit will be unable to send or receive emails.
- Users required to maintain email for more than 180 days should archive, export to PDF, or print and save these emails as needed.

- 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.
- 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.

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 in spite of filtering. ORS cannot assume any liability for such breaches of the filter.
- Use a secure password for your email account. Suggestions include:
    - 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.

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

Web Publishing

ORS users with access to Web 2.0 products as part of their job duties, including but not limited 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 Web 2.0 products 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. Personally identifiable information examples include home and/or school address, work address, home and/or school phone numbers, full name, social security number, etc; no personally 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 post only information that will be useful to and appreciated by the community/network.

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 has created and hosts options for teachers to safely use social media for instructional purposes. As part of these options, 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.
- 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 or "fan page's" creator or of his/her opinion, product, or service. The same applies to comments posted by others to the ORS social media accounts.
- ORS must approve all ORS professional social media accounts bearing an ORS logo and the account users must adhere to the following guidelines:
    - Approved naming convention for all social media accounts as determined by the Director of Technology.
    - Provided list of all requested users of ORS social media accounts. Users must be approved by the Director of Technology and/or the designated 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 user name, 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
    - 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.
- 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.
- ORS approved users of social media are expected to carry themselves professionally and represent ORS positively at all times.
- ***A professional social media account is encouraged to be set up instead of "friending" or "following" personal accounts.*** A potential danger exists when employees communicate directly with students or instruct students to communicate directly to each other or the general public on social media sites that are not hosted by ORS.
- It is strongly recommended that teachers do not "friend" or "follow" current students and/or students under 18 years of age. There may be exceptions, such as a relative, a friend's child, etc.; however, as a general rule, it is recommended that teachers do not "friend" or "follow" students and that they assume personal responsibility if they choose to do so. ***It is recommended that employees should establish separate social media accounts for personal and professional purposes.***
- 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.

Additional Recommendations:

- Remember, once something is posted on a social networking site, it may be available forever.
- Avoid posting comments that discuss or criticize others.
- Only post what could be shared in a face-to-face meeting with the public (e.g., no confidential student information).
- Make sure posts and pictures are presented in a professional role or manner and in accordance with ORS media release procedures.

Netiquette

- In email and postings on websites, be polite and use civil language – no cursing or swearing or vulgarities, suggestive, obscene, belligerent, or threatening language.
- 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.
- Do not respond to inflammatory or inappropriate messages by any means.
- Always delete email or other messages from unknown or untrustworthy senders, suspicious files, links, or URLs. These can contain malicious software or viruses.
- 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.
- 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 provided 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.
- Use a signature on the bottom of your email in which you identify your name, phone number, job title, and location.

Information Technology Acceptable Use

Examples of acceptable use include activities outlined in the following list:

- All IT resource accounts are to be used only by the authorized owner of the account for authorized purpose.
- Email and internet access is to be used for official purposes and limited personal purposes that facilitate the employee's or contractor's maximum availability without interruption of normal work activities (e.g., personal email communication).
- All communications via ORS IT resources should be assumed to be public record and, barring a privilege, can be disclosed.
- Email messages between staff and students should only be used to facilitate classroom learning.
- Parent communication through group email notifications should be sent with the parents' information hidden (e.g., addressing them in the blind carbon copy (Bcc) field).
- Email messages to large distribution groups or school system-wide should not be replied to using the "Reply All" feature.
- All email and internet usage is logged and subject to monitoring by ORS' district IT resources operations and management personnel and through automated means for inappropriate, impermissible, or illegal activity.
- Any suspected illegal or non-approved use of ORS IT resources shall be reported to the ORS IT department immediately.
- Users are responsible for protecting their IT resources accounts credentials, particularly passwords for gaining access to the ORS data network, email, software, systems, and other accounts. Login and password information should never be shared, with the exception of ORS district-level officials and Technology Support Technicians

who have cognizance over systems for which a user requires technical assistance.

- Users accept the responsibility for all material sent from and/or stored in their account.
- Users will not download copyrighted software, inappropriate text, and/or graphic files or files dangerous to the integrity of the network.
- Users will regularly delete electronic messages and any unnecessary files to limit storage space being utilized by their account.
- All unattended computing equipment will be password protected (e.g., screen locked, logged off, etc.).
- Students should NOT be allowed access to a teacher's computer except for classroom demonstrations on the projected screen while under the supervision of the teacher.
- Users have the responsibility to report inappropriate use of the network and violations by others to their immediate ORS administrator.

Information Technology Unacceptable Use

Examples of prohibited activities include, but are not limited to, the activities outlined in the following list:

- Any use of ORS IT for any unlawful purpose is prohibited.
- Revealing others' personal information, such as an address or phone number, without auditable record of authorization is prohibited.
- Any use of ORS IT for individual profit or gain is prohibited.
- ORS IT shall not be used for product advertising or political activities.
- Excessive use of ORS IT for personal business is prohibited.
- Any activity that serves to disrupt the use of IT by other users is prohibited.
- Users shall not destroy, modify, or abuse any ORS IT hardware or software, including circumventing internet content filters or network safety measures.
- Malicious use of ORS IT resources to develop programs for the use of harassing other users, infiltrating computers or computing systems, or altering or damaging software is prohibited.
- Any unauthorized installation of any software, including shareware and freeware, for use on ORS district's network is prohibited.
- Users should not compose, send, or attach any defamatory, inaccurate, abusive, profane, sexually-oriented, threatening, racially offensive, or illegal digital messages, documents, or files. This includes school or district-wide email messages derogatory of the abilities and/or actions of other employees/contractors. Complaints should be directed to and handled through ORS Human Resources.
- ORS IT users shall not contribute to or further propagate hate mail, chain letters or messages, harassment, discriminatory remarks, or other antisocial communications.
- Visits to websites containing profane, sexually-oriented, threatening, racially offensive, or other objectionable material are prohibited.
- Downloading, copying, otherwise duplicating, or distributing copyrighted materials without the specific written permission of the copyright owner is prohibited. 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).

- Revealing or communicating students' personally identifying or sensitive information or students' academic or assessment work via email or other means using ORS IT resources is prohibited without written consent by the student's parent(s)/legal guardian(s).
- The same relationship, exchange, interaction, information, or behavior that would be unacceptable between a staff member and a student in a non-technological medium is unacceptable through the use of technology.
- Login and password information shall not be shared except to facilitate diagnoses and resolutions of IT hardware or software problems or failures as may be necessary by responding to bona fide ORS IT personnel or other district-level employees who have management cognizance over systems.
- Playing games using ORS IT resources, unless specifically authorized for educational purposes, is prohibited.
- Using a computer account not authorized for use is prohibited.
- District staff are prohibited from accessing personal social networking sites on school computers or during school hours except for legitimate instructional purposes.

Applicable Laws

- FERPA: www2.ed.gov/ferpa
- CIPA: http://www.fcc.gov/guides/childrens-internet-protection-act

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 reported by ORS officials to the appropriate law enforcement officials.

Oak Ridge Schools Education Network NetID Application/Renewal
Acceptable Use Policy & Internet Safety Agreement (Non-Student}

Return to the Human Resources department.

Please circle all that apply:

New NetID Application/AUP Renewal Previous ORS Employee (Yes/No) Teacher Licensed (Yes/No)

_____
Print Full Legal Name (exactly as printed on your Social Security Card)

_____
Preferred Name (e.g., Bob instead of Robert or middle name) Date of Birth

_____
Primary Building Assignment / Room # / Department Position

I have read and understand the Acceptable Use Policy for accounts on the Oak Ridge Schools Education Network. I agree to abide by these policies and procedures. I understand that accounts and network usage are subject to review by Oak Ridge Schools' administrators and that any misuse will be referred to officials for appropriate action.

_____
Signature Date

If you are requesting a new NetID, you will receive a notice via inter-office school mail alerting you when your account has been created. This usually occurs within five business days after turning in your Oak Ridge Schools Education Network NetID Application.

APPROVAL

_____
Signature of Director/Principal/Supervisor Date

_____
Signature of Human Resources Representative Date

ADMINISTRATIVE USE ONLY

Date Received: By: Incident #:

Date Created: By: NetID:

On File: Technology Department Document Imaging