Oak Ridge
SCHOOLS

Technology Acceptable Use Policy & Device Use Policy

ORTN Account Users

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

Index

1. Introduction

Oak Ridge School District (ORS) is committed to providing access to local, national, and international sources of information and fostering an atmosphere that encourages knowledge sharing. The district assumes that information resources will be used by its community members in accordance with established guidelines and regulations. This policy aims to create an intellectual and reasonably secure environment where students, faculty, and staff can collaborate both within ORS and with other institutions. It supports the district's goal of fostering academic freedom while respecting freedom of speech and privacy rights. Reasonable steps will be taken to protect intellectual, creative, and professional efforts from misrepresentation, tampering, destruction, and theft, although absolute security cannot be guaranteed.

This policy defines acceptable use of ORS's technology resources, including computers, data, networks, software, Internet, email services, telephone services, computer labs, and technology classrooms. These resources are to be used for school-related purposes. This policy applies to all users of ORS technology resources, whether they are affiliated with the district or located on or off campus. All said users are responsible for adhering to the district's Acceptable Use Policy. Violations may result in penalties, including expulsion, dismissal, or revocation of user access. Access to technology resources is a privilege, not a right, that may be revoked at any time.

2. Purpose

The purpose of this policy is to outline the acceptable use and care of technology resources at ORS, ensuring their proper function and protecting the integrity of ORS network and data.

3. Definitions

Oak Ridge Schools Network Identification **(ORS NetID)**
: The account assigned to an employee or ORS affiliate for access to ORS data.

Multi-Factor Authentication **(MFA)**
: A multi-step account login process that requires users to enter more information than a password. For example, along with the password, users might be asked to enter a code sent to their authenticator application, answer a secret question, or scan a fingerprint. Authenticator applications used by ORS are Google, Microsoft, and/or Rapid Identity.

Classroom-Assigned Technology
: Technology that does not leave the classroom/building but is assigned to a staff member. Examples include a newline panel, projector, desktops, and/or wireless access points. Classroom-assigned technology should never be removed from the classroom or loaned to another employee unless approved by the Technology Department.

Staff-Assigned Technology– Technology devices assigned to a staff member or associate of ORS and can be taken outside the building. These devices are used solely by the staff member and never by students.

Computer Equipment Loan Agreement **(CELA)**
: A signed agreement between staff and employees acknowledging the technology assigned to the employee.

Production vs Non-Production Laptops

- *Production Laptops*
  Production devices are assigned to administrative and certified staff for student teaching. A production device will have the guarantee of quick repair/replacement and compatibility with classroom technology and district level software.

- *Non-Production Laptops*
  These laptops are usually assigned to support staff that need a device to perform job functions but are not used for the teaching and learning process. These machines are typically comprised of former production laptops.

Family Educational Rights and Privacy Act (**FERPA**)

Protects student educational data including demographic information, grades, disciplinary actions, extra-curricular activities information, student IEPs, economically disadvantaged classifications, 504 plans, court case or other legal information/records, etc.

Personal Information Definition (**PII**)

An individual's first name or first initial and last name, in combination with any one or more of the following data elements: social security number; driver's license number; or account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. PII does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted or otherwise made unusable.

Personal Health Information (**PHI**)

PHI is considered any data pertaining to an individual's medical conditions or care. This includes medical history, lab results, physical health records, biometrics, etc.
***Please note that finger scanners and facial recognition used by Oak Ridge Schools do not store biometric information. ***

Children's Internet Protection Act **(CIPA)**

Addresses concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA and provided updates to those rules in 2011.

Family Educational Rights and Privacy Act **(FERPA)**

A federal law that affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records.

Childrens Online Privacy Protection Act **(COPPA)**

A federal law that imposes specific requirements on operators of websites and online services to protect the privacy of children under 13.

Protection of Pupil Rights Amendment **(PPRA)**

Governs the administration to students of a survey, analysis, or evaluation.

Health Insurance Portability and Accountability Act **(HIPPA)**

National standards to protect individuals' medical records and other individually identifiable health information (collectively defined as "protected health information") and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization.

Non-Disclosure Agreement - **(NDA)**

An agreement which defines information that the parties wish to protect from dissemination and outlines restrictions on use.

ORS Sensitive Data

Any data that is defined with compliance laws like PII, PHI, FERPA, and all those listed above.

Class I Sensitive Data

- Demographic information
- Grades
- Disciplinary actions

- Extra-curricular activities information

Class II Sensitive Data

- Student IEPs
- Economically Disadvantaged classifications
- 504 plans
- Court case or other legal information/records

4. Compliance and Data Governance, Reporting, and Copyright

Compliance Laws

Laws that govern our data in education are:

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
HIPPA: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Reporting

If you have a breach of your account or feel there was unauthorized access to ORS Sensitive Data, you must report it immediately to your building technician.

Tenn. Code § 47-18-2107 – A breach of PII Any Entity to which the statute applies shall disclose any breach of the security of the system to any resident of TN whose PI was, or is believed to have been, acquired by an unauthorized person. “Unauthorized person” includes an employee of the Entity who is discovered by the Entity to have obtained personal information and intentionally used it for an unlawful purpose.

The disclosure shall be made immediately, but **no later than 45 days** from the discovery or notification of the breach, unless longer is required due to law enforcement's legitimate needs.

Copyright

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

- 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);
- Copyright is implied for all information (text, data, and graphics) published on the internet. Do not "borrow" icons, sounds, or graphics from other pages without documented permission; it is the employee’s responsibility to secure proper usage permission. 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.

5. Data Handling, Loss Prevention, and Protection

Faculty and staff are responsible for using their assigned technology device according to school and district policies, as well as caring for said device in accordance with listed best practices. Employees should not lend their device to another employee or individual.

Security Tips and Passwords
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.

An ORS NetID account operator may be asked to use a form of MFA that requires an application on their personal use device.

Avoid using your ORS NetID credentials on personal or non-educational websites. If you must use your ORS NetID username, make sure to use a different password.

Email
Each ORS NetID provides access to the ORTN.edu domain and ORTN.edu email post office. All messages within the email system are the property of Oak Ridge Schools. Personal use of email is permitted if it is limited and does not violate ORS policy, guidelines, 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.

Email General Guidelines
Any emails about ORS business 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] and adhere to the Employee Code of Conduct.

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 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.
- Always delete email or other messages from unknown or untrustworthy senders, suspicious files, links, or URLs. These can contain malicious software or viruses.
- Stay alert for suspicious emails requesting login information or containing external links.
- Please note, the Technology Department will never send a request for ORTN login via link.
- Always check that recipients of an email may have access to any information contained in that email.

Email Encryption
It is not permitted to send personal, identifiable information about staff, students, or families outside of the ORS email system without password protection/encryption. See instructions for proper email encryption located in our Tech Tips portal at www.ortn.edu/technology.

When password-protecting/encrypting a 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.

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 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.
- Account holders must promptly delete any emails containing ORS Sensitive Data once this data is no longer relevant or needed. The Technology Department will periodically send reports to account holders who have ORS Sensitive Data older than six months to remind them to remove any unnecessary and discoverable sensitive information.

Email Spam
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.

Data Backup
ORS NetID users will have their data automatically backed up through OneDrive, which syncs their profile information with their Office 365 account. To verify the status of OneDrive, users should click on the cloud icon located in the bottom right corner of the task bar.

Data Access
Various positions within Oak Ridge Schools require differing access to ORS Sensitive Data. ORS NetID account holders are expected to follow all local, state, and federal laws in addition to this Acceptable Use Policy regarding the protection of student and staff confidential data.

Unless required to complete job functions, ORS Sensitive Data must not be stored on ORS technology devices in any capacity.

If an employee's position requires access and use of sensitive data, please see guidelines below for storing, sharing, or transmitting ORS Sensitive Data.

This data should always be encrypted and stored in a zipped file or password-protected PDF.

The employee understands that any data (documents, passwords, email, or other form) obtained during the performance of work duties must remain confidential. ORS Sensitive Data should NEVER be stored on personally owned technology or non-ORS technology devices.

Any hard copies 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 liability in any legal action arising from such a breach.

District or school data, such as Skyward student information, accessed through school system technology resources may not be used for non-ORS educational activity. 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 is prohibited as is trespassing in another's folders, work, or files.

If you are an independent contractor for the district, all data pertaining to Oak Ridge Schools must be permanently and immediately removed from any devices not owned by ORS and ORS technology must be returned promptly upon severance of the business relationship with Oak Ridge Schools.

Unauthorized access to ORS data that is stored or managed by non-ORS technology may not fall under ORS insurance coverage, potentially requiring the employee or contractor to compensate for any resulting damages.

Requests for Data Cleanup

The Technology Department may request a staff member to remove specific data from inboxes, OneDrive, technology device, etc. in accordance with their position's data security classification and privileges. The employee is expected to respond or comply to the request within 3 business days.

Student Data Non-Disclosure

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 and any other information otherwise marked or known to be confidential. Staff members should avoid rostering or transmitting student data within unauthorized applications.

Any unauthorized release or carelessness in the handling of confidential information is considered a breach of the duty to maintain confidentiality. Any breach of the duty to maintain confidentiality is grounds for disciplinary action (up to and including immediate dismissal) and liability in any legal action arising from such breach.

If you have questions about student data or specific circumstances, please contact the Director of Technology for clarification.

6. General Rules / Best Practices

All users are expected to use good judgment and to follow the specifics and spirit of this document: be safe, appropriate, careful, and kind; do not try to circumvent technological protection measures; use common sense; and ask if you do not know.

Best Practices
To keep the network and district data as secure as possible, the following best practices should be followed:

- Do not sign into any external website with an ORTN login credentials (username and password)
- Never store sensitive data on a Google Drive or within any other Google file
- Utilize services provided by ORS such as SharePoint, Teams, or other district-approved applications to store data.
- All unattended computing equipment should be password protected (e.g., screen locked, logged off, etc.). Students should NOT be allowed access to a staff issued device.
- Because security needs and functionality changes regularly, it is best practice to test technology associated with lesson plans of time. This will ensure your lesson goes as intended.
- Printing will automatically be set to black and white. For larger print or copy jobs, use the larger copiers to save on costs.

Artificial Intelligence
Staff and students should always abide by the Oak Ridge Schools district Artificial Intelligence Policy.

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 or other personal demographic information will appear with any student likeness except for recognition for honors or awards with parent/guardian consent.

Social Media

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. Approved users are always expected to carry themselves professionally and represent ORS positively.

Please note that any "liking," "linking" 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.

ORS professional social media accounts must adhere to appropriate password procedures listed prior in this agreement.

District sponsored sites such as Canvas, Skyward, and ParentSquare 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 reserves the right to monitor and conduct random "spot checks" to ensure compliance with social media guidelines. 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.

Inappropriate conduct includes, but is not limited to, the following:

- Revealing others' personal information, such as an address or phone number, without auditable record of authorization;
- Creating or storing unauthorized copies of ORS files or data;
- Violating student privacy by sharing personal information that goes against Personal Identifying Information (PII) rules and regulations;
- 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;
- 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;
- 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;
- Any use of technology that represents a violation of the Oak Ridge Schools Employee Code of Conduct

Internet Use and Web filtering (CIPA)
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.**

Like all K-12 districts, compliance with CIPA (Children's Internet Protection Act) is required, and part of that compliance means we use iBoss to filter certain websites considered inappropriate for students. Keep in mind that staff and students have different filters associated with their accounts.

To allow staff to check the current categorization of a specific website address to see if the site may be blocked or whether students have any issues accessing, a Clever link to a Self-Service URL Lookup. Instructions on using this tool can be found here.

Internet activity will be monitored, along with other aspects of technology usage. Internet access for all users is filtered through a web content filtering software in which the Uniform Resource Locator (URL) (web address) and 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.

7. Device Care, Repair, and Tips

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

Computer Equipment Loan Agreement (CELA): Upon receiving an Oak Ridge Schools technology device, staff members will sign and return a Computer Equipment Loan Agreement (CELA) form. The accuracy of the equipment assigned to you on this form is necessary, so please read it carefully.

Returning a Technology Device: Upon resignation or termination, all technology equipment must be returned and accounted for by the Technology Department prior to the employee’s last day of employment or within 5 days of administration request. Failure to do so will result in a filed police report and withheld wages until device(s) are returned.

Care and Maintenance
- Devices should NEVER be picked up by the lid.
- When carrying the laptop, it is expected that the device will be placed in a backpack, bag, or other carrying case.
- Technology devices should be kept at room temperature and should NOT be exposed to extremes of heat or cold. DO NOT LEAVE the technology device IN AN AUTOMOBILE.
- Liquids and food should not be used/consumed near the technology device.
- Cleaners, sprays, alcohol, ammonia, or abrasives should not be used on the technology device. Devices should be cleaned with a soft, lint-free cloth.
- The device should remain in the protective cover when not in use.

- Device should not be in a place where someone could accidentally sit or step on it. Always unplug the device charger when not in use and place it in a safe place away from pets. Devices can be a tripping hazard when charging.
- Faculty and staff should not write on, draw on, or add stickers to any equipment.

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 life.

- ***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 staff-assigned technology device or classroom-assigned 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 staff-assigned technology device or classroom-assigned device issued to the employee.

Employees have accepted responsibility for the technology device and are liable for 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.

Penalty Damage Matrix
Please see the matrix below for costs associated with replacement technology accessories. 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 & Equipment	
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
Other Issued Items	
Alertus Pendant	$10 replacement cost

Non-Production Machines & Equipment	
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.

Employee-Provided Equipment

Any technology equipment in an employee's office or classroom that has been purchased by the employee (keyboard, mouse, special monitors, etc.) must be tagged by the Technology Department while the equipment is used in the building. This is for insurance purposes. Any personal equipment that an employee does not want to be tagged with an ORS sticker should be taken from the building.

8. Acknowledgements

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.

Expectation of Privacy

To maintain network integrity and ensure the network is being used responsibly, school Innovation Coaches, Technicians, and/or other designated staff reserve the right to inspect 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 using 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 (Tennessee Public Records Act). 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 all files stored on the network, on individual computers, or storage media to assure compliance with ORS policies and state and federal laws. ORS has the right to gather electronics for disposal or investigation at any time.

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.

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.
The system-wide technology staff performs routine backups 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.

Each employee agrees to take all reasonable steps to help ensure the security of the Oak Ridge Schools network including Multi-Factor Authentication measures.

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

ORS Net ID holder (each employee, contractor, sponsored account or other) 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.

Failure to comply with an equipment return request from ORS may result in the forfeiture of funds needed for its replacement, if feasible, and/or a theft report being filed against the individual responsible.

Signature

Employee Name (Printed) _____

Employee Signature _____ Date: _____

Official signature for this document must be done electronically. Any physical copies are to be used for reference only. This agreement is on the Oak Ridge Schools website.