SUBJECT: EMPLOYEE ACCEPTABLE USE OF DISTRICT TECHNOLOGY

Purpose

Onteora Central School District (OCSD) encourages use of the District Computing Systems (DCS) to explore educational topics, conduct research and engage in work-related professional communication to further the mission of OCSD. It is anticipated that access to various electronic information resources will expedite and enhance the performance of work-related tasks and assignments.

Use of the DCS shall cease and the equipment returned to OCSD or the user's access revoked under any of the following circumstances:

1. A user separates from service as an employee of OCSD.
2. Status as a person authorized to access the DCS or use OCSD equipment terminates.
3. A user is assigned a new position and/or responsibilities pursuant to which use of the DCS, or a portion thereof, has not been authorized.
4. User violated this policy.

Anyone who is aware of any misuse or abuse of any software or electronic communication system owned or leased by OCSD shall notify his/her immediate supervisor or building principal.

An administrator who is aware of any misuse or abuse shall notify the Superintendent, Assistant Superintendent, or designee, and appropriate disciplinary action may occur based on the circumstances and in accordance with all applicable laws, bargaining agreements, Board policies, and administrative regulations.

User Responsibilities

Each user of the OCSD systems and/or services shall submit a signed Technology Acceptable Use Agreement Form to acknowledge the receipt of this policy and its accompanying regulation

With increased concern about identity theft, unwarranted invasion of privacy and the need to protect personally identifiable information, prior to students being directed by staff to use any cloud-based educational software/application, staff must get approval from the Building Principal and Director of Technology. The Building Principal and Director of Technology will determine if a formal contract is required or if the terms of service are sufficient to address privacy and security requirements, and if parental permission is needed.

See Regulation 6470R

Adopted: 8/14/18

Onteora Central School District
Regulation Number: 6470R
Technology Acceptable Use Employee Agreement
Onteora Central School District
Date: June 19, 2018

---

1. SCOPE AND DEFINITIONS

The intent of this policy is to make clear the responsible use of the Onteora Central School District network and technology systems, not to exhaustively enumerate all possible violations. For purposes of this policy, the district shall consider any of the following subject to the use provisions and limitations defined in this policy:

- file servers, network connections, data lines, infrared nodes.
- desktop computers, printers, laptops, tablets, docking stations, desk or wall data jacks.
- district owned software.
- projection units, smart boards, video cameras, Apple TVs, televisions, monitors, projection screens, speaker systems and microphones.
- phone I voice systems, including voice mail, wall and desktop handset equipment.
- library or other security devices including scan devices, cameras, access control modules, keypads, monitors.
- any other technology equipment available to employees.

2. PROFESSIONAL I EMPLOYEE RESPONSIBILITY

Data, Video and Voice networks have been provided by the "District" as a valuable tool and a necessary component of an employee's work. In addition, varying work responsibilities result in access to information sources such as software, programs, Internet, district data networks etc. Although employees may have access to these information sources, their use may be restricted. Therefore access and authorization to network or web based district information and technology equipment shall carry a corresponding responsibility within the scope of each employee's responsibilities to their appropriate use as defined within this policy. District equipment and access is intended for use solely to conduct educational and professional I career development activities. It is the employee's responsibility to restrict his/her use of said technologies and information resources to these purposes.

3. PRIVILEGES:

The use of the electronic information systems is a privilege, not a right. Inappropriate use may result in cancellation of an employee account, and I or other disciplinary actions tailored to meet the specific concerns related to the violation.

4. ACCEPTABLE/ UNACCEPTABLE USE:

A. Access rights, employee accounts, and passwords are assigned to individuals. Employees are advised not to provide others with his/her access privileges for use of district systems. Please be aware that any employee may be held responsible for the actions conducted from or data generated/saved/manipulated within his/her user account.
B. Any use that is illegal or in violation of Board policy, including, but not limited to, harassment, discriminatory or threatening communication and behavior; violations of copyright or other laws is prohibited.
C. Engaging in commercial activities including but not limited to the promotion of a personal business, financial gain, advertising or solicitation purposes shall be considered a direct violation of this policy.

D. All users are expected to take reasonable precaution to secure district information stored on devices they use, including maintaining responsible custody over computer resources, ensuring no unauthorized use of district devices, and exercising prudent judgement when browsing the internet and opening emails.
E. Any use as a forum for communicating by e-mail or any other medium with other school users or outside parties to solicit, proselytize, advocate or communicate the views of an individual or non-school sponsored organization; or to raise funds for any non-school sponsored purposes, whether for profit or not-for-profit, is prohibited. This list is provided for illustrative purposes only and is not intended to be all-inclusive.
F. Any use involving materials that are defamatory or sexually explicit are prohibited
G. Any communication with students or minors that is not age appropriate or appropriate for a student-teacher relationship is prohibited
H. Knowingly providing school e-mail addresses to outside parties whose intent it is to communicate with school employees, students and /or their families for non-school purposes is prohibited.
I. Intentionally opening or forwarding any e-mail, attachments or other files from any source that is known to contain a virus or viruses is prohibited.
J. It is prohibited to access, send or download any of the following: pornographic, obscene, profane, lewd, vulgar, rude, inflammatory, threatening materials.
K. Technology resources are expensive to maintain and operate. It shall be each employee's responsibility to use district systems and supplies judiciously and at all times in accordance with this policy. Spilling food and/or drinks on District equipment or other actions which compromise the District's equipment should be avoided.
L. Modifications to hardware, networks or software is prohibited. Additionally, employees and or students do not have a right to load software on any district system. Any new software should be requested through the Building Principal and purchased through the Technology Department. Software will then be loaded by the Network Technology staff.

5. COPYRIGHT:
It is the employee's responsibility to adhere to all copyright laws related to print, data or video use.

6. STUDENT PERSONAL SAFETY:
A. Employees who supervise students with use and access to "Technology Systems" shall be familiar with the Onteora Central School District Student Use Policy Agreement and enforce all of its provisions.
B. Employees with access to student records may not use, release, or share these records with any third party, including but not limited to individuals, third party vendors or cloud based platforms without the authorization of the Onteora Central School District.
C. All Student "technology systems" use will be supervised by a responsible staff member. It is the responsibility of the staff member supervising students to report any resulting misuse by their students to the building administrator.

7. SYSTEMS SECURITY:
A. Employees are responsible to insure the security of any district technology equipment, files, information, data, passwords assigned to or created by them
B. Employees with access to student records may not use, release, or share these records except as authorized by the Onteora Central School District, and /or Federal or State Law.
C. Once an employee has "signed on" and accessed a district network, he/she shall not leave the room with the workstation unattended at any time without utilizing a password protected screen saver. The passwords must be registered with the technology department so that they are able to access computer

if needed.

D. Employees should shut down and power off equipment at the end of the work day.

8. EMPLOYEE LIABILITY:

A. Employees may not move any equipment from the room where it is assigned or reconfigure any of the technology/network resources, which may result in damage or unnecessary "downtime" to any district data, video or voice system and/or component. It shall be the employee's responsibility to secure appropriate permission to move, adjust, or reconfigure such resources and arrange for assistance from the Network Technology Staff.

B. Employees assigned "technology equipment" are responsible for its basic care and safety. Any damage to equipment or other issues with equipment must be reported immediately.

C. It shall be each employee's responsibility to report any attempts or actions of a person to vandalize, degrade or disrupt technology equipment or system performance.

D. All employees who utilize school computers for instructional purposes with students have a duty to supervise and monitor online activities of students while in school, including but not limited to use of e-mail, chat rooms and other forms of direct electronic communication, "hacking" and other unlawful activities of minors, and access to materials harmful to minors. Such employees must be familiar with the school district's policies and rules concerning student computer and Internet use and enforce them. When, in the course of their duties, employees become aware of student violations, they shall stop the activity and inform the building principal (or other appropriate administrator) immediately.

9. EXPECTATION OF PRIVACY:

A. Employees shall have no expectation of privacy in files, disks, drives, documents, electronic mail, which has been created in, entered in, stored in, downloaded from, or used on district equipment and systems, and is subject to Freedom of Information Law (FOIL).

B. Electronic mail has been provided for correspondence and communication as related to your employment in an educational environment and not for personal business use. The district understands that occasional personal communication may occur. However, the district reserves the right to determine when such use is excessive and in violation of this policy.

10. SERVICES AND ASSUMPTION OF RISKS:

A. The district makes no warranties of any kind, whether express or implied, for services provided and is not responsible for any damages suffered while on the systems, to include loss of data, inaccurate or poor quality information, and missed-deliveries, or service interruptions caused by the system or by your own errors or omissions.

B. The district reserves the right to remove files, limit or deny access, and refer staff for other disciplinary actions in accordance with this policy.

C. The district reserves all rights to any material (voice, data, and video) stored in files, drives or other storage means owned by the Onteora Central School District.

D. The district and/or network resources are intended for the exclusive use by their registered users. Staff is responsible for the use of his/her account/password and/or access privilege. Any problems which arise from the use of a staff account are the responsibility of the account holder.

Best Practices for Wi-Fi Devices

1. Turn off the device when not in use and at the end of each day.
2. If device is to stay on, turn Wi-Fi off when not in use.
3. Always place the device on a solid surface.
4. Viewing distance should be a minimum of 12 inches from the screen.

I hereby acknowledge my responsibilities to act in accordance with this Employee Acceptable Use Agreement. I understand that if I am found to be in violation of any provisions in this Regulation/Agreement or in Policy 6470, it may result in my being subject to disciplinary action, the revoking of my account(s), the collection of equipment I software assigned to me, personal financial liability and I or appropriate legal action.

Your signature on the sign-in sheet titled “Attendance of Mandatory Training & Acknowledgment of Policies” on September 4, 2018 includes this regulation