

Okemos Public Schools

4406 Okemos Road
Okemos, MI 48864

Acceptable Use Policy ***District Network Resources and Internet Safety***

The Okemos Public Schools (OPS) encourages staff, students, parents and the community to utilize technology resources. The OPS District Network Resources which include voice, video, data, Personal Learning Devices (PLD) and Internet networks, is maintained by the Department of Media & Technology. These technology resources are valuable tools for access to and the delivery of information, learning and communication. All users of these technology resources have the responsibility to use them properly. The use of the District Network Resources must be in support of education and consistent with the purposes, curriculum and mission of the Okemos Public Schools.

All technology resources are the property of the district and the district retains the right to access and review all computer files, electronic mail and Internet access. It is expected that all users of technology resources will maintain a high standard of ethical behavior. Inappropriate use may result in suspension of privileges, cancellation of privileges, disciplinary action and/or legal action. The notification for students of the Acceptable Use Policy (AUP) of the District Network Resources and Internet Safety will be provided annually in the Parent/Student Handbooks. Employees must sign the District Network Resources and Internet Safety Employee Contract before their network account can be accessed. The signature on the Employee Contract is legally binding and indicates the party who signed has read the following Terms and Conditions for Use of the Acceptable Use Policy carefully and understands their significance.

Terms and Conditions for Use:

Computer Network:

- A network account is provided for ***educational purposes only***.
- Acceptable Network use by district students and staff include:
 - Creation of files, digital projects, videos, web pages and podcasts using network resources in support of education and research.
 - Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, email and web pages that support education and research.
- A network account is to be used only by the authorized user. The sharing of logins, passwords or accessing another user's account and/or data is prohibited.
- Users are expected to abide by the generally accepted rules of Network Etiquette (Netiquette) including:
 - Be polite. Do not send abusive messages or ones containing inappropriate language.
 - Do not reveal your personal information (address, social security number, phone number, etc.) or that of other students/colleagues.
 - Do not wastefully use finite resources (paper, network/email storage space, etc.).
 - Do not use the network in such a way that you would disrupt the use of the network by others.
- Email/Social Media/Messaging may not be used to spam, advertise/sell personal property, for commercial activities, or for political lobbying for personal gain. Messages relating to or in support of illegal activities will be reported to legal authorities.
- Uploading, downloading or transmission of material, information, or software in violation of any district policy or federal, state or local law or regulation is prohibited and may be reported to legal authorities.
- Users may access educational materials for school use via the Internet. Compliance with Copyright notices and/or Terms and Conditions pertaining to a Website is required. Plagiarism, in any form, is prohibited.
- Non-educational, inappropriate communication including, but not limited to, instant messaging, network messaging, and chat rooms, is prohibited.
- Accessing, transmitting, submitting, posting, publishing, or displaying any inappropriate or illegal material including, but not limited to, defamatory, inaccurate, abusive, obscene, profane, sexually oriented, bullying, threatening, racially offensive, or harassing, is prohibited and may be reported to legal authorities.
- Student network files may be purged at the end of the school year. It is the student's responsibility to back up any files he/she wants to retain.
- The network account, email account and network files of a user who leaves the district may be deleted. It is the user's responsibility to back up any files he/she wants to retain.

- The Children's Online Protection Privacy Act requires website operators to obtain parental consent before collecting information from children under the age of 13. In certain instances, the District may act as an intermediary and provide the required parental consent on behalf of a student when the website is used for educational purposes.
- A staff member wishing to design and publish a website must read and adhere to the district's Web Page Development Guidelines and Policy.

Equipment:

- The user will utilize district hardware (computers/printers/scanners, etc.) with care. Food, drink and candy must be kept away from any hardware.
- To protect logins/files, users must restart or shut down the computer after use or when the computer will be unattended for a period of time.
- Users are always responsible for their assigned device. Users must take appropriate security measures at all times such as setting a passcode and/or logging out when necessary.

Security:

- It is the responsibility of every user to notify a staff member or administrator who, in turn, must notify the Department of Media & Technology if the District Network Resources policy violation or security problem involving the District Network Resources or Internet is identified. The user must not in any way communicate and/or demonstrate the problem to others.
- Attempting to login to the network as any other user or disclosing another user's login and password is prohibited.
- Any user identified as a security risk or having a history of technology violations may be denied access to the District Network Resources.

Software:

- Downloading of unlicensed, malicious, illegal or inappropriate software from the Internet is prohibited and may be reported to legal authorities.
- Unauthorized copying, use or altering of licensed or copyrighted software is prohibited.

Tampering:

- Tampering with, or activities that threaten, the integrity and/or security of any network, computer operating system, software or materials (including, but not limited to, hacking into the District network(s), downloading or installing files that will compromise the network(s), dual booting devices, removal of district computer policies, removal of anti-virus software, transmission of worms, viruses and other malicious codes, and accessing any device or data without proper authorization) is prohibited and may be reported to legal authorities.
- Any attempt to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited (e.g., proxies, https, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content).

Internet Safety:

- In compliance with CIPA (Children's Internet Protection Act passed by Congress on 12/15/00) Internet filtering is in place for every networked computer to prevent access to inappropriate material on the district network. Internet filtering is provided by the district, both in and outside of the school setting for students. It is impossible to control access to ALL material on the Internet. The OPS firmly believe that the availability of valuable information and the potential for interaction on the Internet far outweigh the possibility that users may be exposed to material not consistent with the educational goals of the Okemos Public Schools. Furthermore, during student Internet use in school facilities, District staff will make reasonable efforts to supervise student access and use of the Internet.
- To help ensure student safety and citizenship in online activities, students and staff will be educated about:
 - Appropriate online behavior.
 - Safety and security while using email, chat rooms, social media, and other forms of electronic communications.
 - The dangers inherent with the online disclosure of personally identifiable information.
 - The consequences of unauthorized access (e.g., "hacking") and other unlawful or inappropriate activities.
 - Cyberbullying awareness and response.

Video Network:

- All programming to be aired over the district's broadcasting system must be approved by the Department of Media & Technology.
- Programming which may be in violation of someone's civil rights, or that is discriminating in nature or content, or inappropriate for the educational audience, is prohibited.
- Inappropriate language or behavior is prohibited from Okemos Channel programming.
- Student programming and use of equipment must be adult supervised at all times.
- Copyrighted materials or programming must be used in accordance with district policy and applicable laws.

Disclaimer: The Okemos Public Schools makes no guarantees of any kind, whether expressed or implied, for the District Network Resources or the device. The Okemos Public Schools specifically denies any responsibility for the accuracy or quality of information obtained through its services. OPS staff and Board of Education members are released and indemnified from:

- Any damages users may suffer including, but not limited to, loss of data resulting from delays, nondeliveries, misdeliveries, interruptions in service, or other reasons.
- Any fees, expenses or damages a user incurs as a result of use, or misuse, of the District Network Resources. The district retains the right to seek monetary restitution from the user.
- Any claims, causes of action and damages of any nature arising from the use, or inability to use, the District Network Resources.
- Unauthorized financial obligations, identity theft or fraud resulting from District-provided access to the Internet and/or email.

Terms and Conditions: All Terms and Conditions as stated in this document are applicable to the Okemos Public School District. These Terms and Conditions reflect the entire agreement of the parties and supersede all prior oral or written agreements and understandings of the parties. These Terms and Conditions shall be governed and interpreted in accordance with the laws of the State of Michigan, and the United States of America. These Terms and Conditions are subject to change with proper notification to the registered users.

Revised 07/19/16