Oak Hill Union Local School District

Acceptable Use Policy

Use

1) **EDUCATIONAL OBJECTIVES**: The use of the district technology resources and Internet access must be in support of education and research and be consistent with the educational objectives of the Oak Hill Union Local School District. Computer access is essential for success in most classes.
2) **ACCESSING, DOWNLOADING or TRANSMITTING OF MATERIALS**: Accessing, downloading or transmitting of any material in violation of any U.S., state, or school regulation is prohibited. This includes but is not limited to: copyrighted material, threatening, abusive, explicit or obscene material, hate mail, chain e-mail, harassment, discriminatory remarks, cyber-bullying, and other antisocial behavior.
3) **EDUCATIONAL USE:** Computers are for educational use, they are not to be used for commercial, political, or illegal activity.
4) **SCHOOL EMAIL**: Staff should not use any other email system for official school communication. Emails related to a school and /or district fall under the public record laws. Private email accounts used for school activities would also be public records. Email is archived on Microsoft's servers. Be careful what you send. The forwarding of chain e-mail is prohibited.
5) **VANDALISM/THEFT**: Acts of vandalism or theft will result in cancellation of all privileges, and be reported to the civil authorities. Students and/or Parents/Guardians of students damaging school property will be held financially responsible for it. Vandalism is defined as an attempt to harm, modify, or destroy any workstation, network, or peripheral device; including but not limited to all software and hardware.
   This includes, but is not limited to, the uploading or creation of computer viruses.
6) **SOFTWARE INSTALLATION**: Only technology staff can install software. Some software may be queued and then installed when the user logs on. Installation of software onto the network or onto individual workstations by end users is prohibited. Only properly licensed software will be installed on district computers. Copying or distributing school or personal software is prohibited by all users.
7) **INAPPROPRIATE MATERIAL:** The Internet consists of computer systems networked all over the world. Users (and parents of users who are under 18 years old) must understand that neither the school nor the District can control all the content and information. Some content may be controversial and/or offensive. Internet safety training is provided to the students. The District has also implemented filtering measures to prevent students from accessing inappropriate materials and monitoring software, which maintains a running log of Internet activity; recording which sites a particular user has visited. Intentionally accessing inappropriate material is expressly prohibited. Accidental offences must be reported immediately to prevent disciplinary actions. Employees, students and parents of students must be aware that the privileges to access online services may be withdrawn from users who do not respect the rights of others or who do not follow the rules and regulations established. A user's agreement is signed to indicate the user's

   (or user's parents) acknowledgement of the risks and regulations for computer/online services use. The District is not responsible for materials acquired on the network.

NETIQUETTE

8) You are expected to abide by the generally accepted rules of network etiquette. These include but are not limited to:
   a. Be polite; keep message brief
   b. Use appropriate language – do not swear or use vulgar language.
   c. Do not use the network in such a way as to disrupt the use of the network.
   d. Report all problems immediately to your teacher or the network administrators.
   e. If you receive a message of questionable content or origin, report this immediately to your teacher or network administrators.
9) Rules and regulations of on-line etiquette are subject to change by the administration.

SECURITY

10) When assigned to an account:
    a. Student passwords are assigned by the District. Staff members need to select a password that is unique and not easily deciphered by others. A password that includes upper and lower case along with numbers is more difficult for others to crack.
    b. Don not tell others your password.
    c. Do not reveal personal home address or phone number or those of other students or colleagues.
    d. You are ultimately responsible for ALL activity under your account.
    e. Do not use another person's password.
    f. If you feel someone else knows your password, please notify the Technology Coordinator and ask that it be changed.
11) Do not circumvent security measures on school or remotely accessed networks.

PRIVACY

12) All files and messages stored on the file server or any workstations are property of the District and may be subject to periodic inspection and deletion. The district reserves the right to monitor and or archive ALL data that passes through the districts computers and/or computer network.
13) Do not consider e-mail as private, as most school email falls under public record laws. Messages sent using wrong usernames or addresses go directly to the person designated as Postmaster for that server and will be read by that person. If desired, school administration can read messages. Once sent, you have no control over what the receiver does with your message. That person may forward it on to other people, but your name will stay encoded with that message as the original sender; therefore, be careful what you write!
    Messages relating to or in support of illegal activities may be reported to the authorities.
14) Software is in use by the district that tracks all Internet and Electronic Mail activity.

PRIVILEGE

15) Use of the network is a privilege, not a right. Inappropriate use may result in a cancellation of privileges, and may result in school disciplinary action and/or legal action to be taken against the user. School Administrators will determine what is inappropriate and their decision is final. The Tech Coordinator may close an account at any time.
16) Students will be given computer network and Internet access unless The District receives a written notification to the contrary. Written notification should be sent to the attention of the Building Principal at the school where the child is in attendance.
17) School District makes no warranties of any kind, whether expressed or implied, for the service it is providing. School District will not be responsible for any damages you suffer. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruption caused by its own negligence or your errors or omissions. Use of any information obtained via the Internet is at your own risk. School District specifically denies any responsibility for the accuracy or quality of information obtained through its services.
18) Conditionally personal devices may be used on the school network. Devices must be registered with the technology department. Additional software or apps may be required to access the network. Compliance with district policies is required, and all network traffic may be monitored. Use of cellular networks or nonschool Wi-Fi to bypass filtering is prohibited. Use of personal hot spots or non-district access points is prohibited. Additional restrictions may be set by the building principals and classroom teachers.
19) All related student-handbook policies apply to computers, computer usage and school networks.

Revision approved [August 16, 2017]
Revision approved [December 20, 2012]
Oak Hill Union Local School District Board of Education