NORTH PANOLA SCHOOL DISTRICT

Acceptable Use Policy (AUP) – Access To Technology Resources

Introduction

The North Panola School District (NPSD) recognizes that technology affects the manner in which information may be accessed, communicated and transferred. Telecommunications, electronic information services, and networked services significantly enhance the learning experience by opening schools, classrooms, and library media centers to a broader array of resources. The district supports access to technology resources for students and staff members in order to further our educational mission, goals, and objectives.

Overview

As the use of telecommunication networks by students and educators increase, there is a need to clarify acceptable use and safety of those networks and to comply with the Children's Online Privacy Protection Act (COPPA) [15 U.S.C. Chapter 91], the Children's Internet Protection Act (CIPA) [47 U.S.C. § 254], and any regulations promulgated under those statutes. This document serves as a legal and binding document for access to any district provided technology resources.

Internet Access

The NPSD provides the privilege of Internet access to district administrators, staff, students, and occasionally guests. Each user, as well as a minor's parent/guardian, willingly agrees to release, hold harmless, defend, and cover the NPSD, its officers, board members, employees or anyone affiliated with the NPSD for and against all claims, actions, charges, losses or damages which arise out of the user's use of the NPSD network or through the use of devices provided by NPSD, whether connected to the NPSD network or not, including but not limited to negligence, personal injury, wrongful death, property loss or damage, delays, non-deliveries, mis-deliveries of data, or service interruptions. NPSD will fully cooperate with local, state or federal officials in any investigation related to illegal activities conducted through the user's account.

Access will be restricted as required to comply with the Children's Internet Protection Act. Web browsing may be monitored and records retained to ensure compliance.

Users are expected to respect the web filter and shall not attempt to bypass the filter when browsing the Internet. Bypassing the web filter through the use of VPN, TOR, or any other programs or applications is prohibited. The determination of whether material is appropriate or inappropriate is based solely on the content of the material and the intended use of the material, not on whether a website has been blocked or not. If a user believes a site is unnecessarily blocked, the user should submit a help desk ticket with the web link and justification of how the site will benefit students academically.

NPSD Network Rules

- The person to whom a NPSD network account is issued is responsible at all times for its proper use.
- Any inappropriate use of the NPSD network may result in the loss of network privileges, disciplinary action, paying for damages, detention, suspension, expulsion, and possible referral to legal authorities.
- Any district employee who uses the NPSD network inappropriately is subject to disciplinary action, including dismissal.
- Under no circumstances should a NPSD network user give their password information to another user nor allow another user to utilize their account unless speaking directly to a member of the Technology Department who is assisting them.
- Schools may supplement any provisions of the District Acceptable Use Policy (AUP) and may require additional parent releases and approvals, but in no case will such documents replace the District AUP unless explicitly stated in such documents.
- Users will immediately report to school district authorities any attempt by other network users to engage in inappropriate conversations or personal contact.
- Any non-standard software that is needed to perform a specific job function will need to be brought to the attention of the Technology Department. Those applications shall be the sole responsibility of that office and if the application interferes with any required programs, applications, and utilities, it should not be used and if in use, it may be disabled.

Acceptable Uses of Technology (not all inclusive)

A responsible user of technology will:

- Use school technology for school-related activities.
- Follow the same guidelines for respectful, responsible behavior online that they are expected to follow offline.
- Treat school technology resources carefully and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.

- Alert a teacher, administrator, or other staff member if they see threatening, inappropriate, or harmful content (images, messages, and posts) online.
- Use District technologies at appropriate times, in approved places, for educational pursuits.

This is not intended to be an extensive list. Users should use their own good judgment when using NPSD technology.

Unacceptable Uses of Technology (not all inclusive)

- Violating any state and/or federal law (including but not limited to copyright laws).
- Using profanity, obscenity, or other language that may be offensive to others.
- Making personal attacks on other people, organizations, religions, or ethnicities.
- Accessing, downloading, storing, or printing files or messages that are sexually explicit, obscene, or that offend or tend to degrade others. The administration invokes its discretionary rights to determine such suitability.
- Not respecting the privacy of a person by posting personal contact information, such as work/home address, telephone, e-mail, photographs, names, or other personal information, without obtaining prior permission from the person affected.
- Posting or transmission outside the NPSD of student without written parent/guardian permission.
- Forwarding personal communication without the author's prior consent.
- Using the Internet for commercial purposes, financial gain, personal business, producing advertisement, business service endorsement, or religious or political lobbying.
- Destroying or altering the files of another user.
- Viewing or taking the files of another user.

Email

Employee and student NPSD email is the property of NPSD. NPSD does not archive employee or student email. It is the responsibility of the employee and student to maintain their email account appropriately.

Use of "Internet mail" by students, staff, and faculty such as Yahoo mail, Gmail, and POP3 accounts by their "home" Internet services provider is allowed unless it does not pass the web filter. The district does not block use of Internet mail accounts, but any "OFFICIAL" communications, e.g., Teacher to Parent, Teacher to Student, Staff to Staff, must be via the district's email system. This includes, but is not limited to teachers who guide extracurricular activities such as Clubs, Bands, Athletics, and the like. This also applies to prohibit the use of messaging in Facebook or other social media services for such official communications.

Filtering

An internet filter is in place for NPSD. The filter is a critical component of the NPSD network as well as Children's Internet Protection Act (CIPA) compliance since it allows valuable online Internet access while restricting access to specific unwanted material in the following categories:

- Ads
- Alcohol & Tabacco
- Auctions
- Games
- Guns & Weapons
- Malware
- Porn/Nudity/Adult Content
- Drugs
- Gambling
- Shopping
- Streaming Radio/TV
- Violence & Hate

This filter updated weekly in order to restrict access to the items above. Filtering is not a 100% foolproof way of limiting access to appropriate sites. Inappropriate sites are added to the Internet daily. Students will be monitored at all times by a teacher or any personnel employed by the NPSD while using the Internet. All inappropriate hits are logged along with the date/time and the IP address of the workstation making the request. Attempts to bypass the school Internet filters is in violation of this AUP and will be subject to disciplinary action that may include denial of access to technology, detention, suspension, expulsion, termination of employment or other remedies applicable under the school disciplinary policy, and state or federal law.

Workstation Monitoring

All data transferred and/or transmitted over the NPSD network can be monitored and recorded at any time. All data transferred or transmitted over the network can be tracked and identified, and originating users can be held liable if their use of the network violates any established policy, regulation, or law. Any data stored on district-owned equipment may be archived and preserved by the district for an indefinite period. Such data includes, but is not limited to E-mail, text documents, digital photographs, music, and other digital or electronic files. If a particular workstation continues to try to connect to an inappropriate site, that workstation will be remotely monitored and the individual using that workstation will be reported to the Principal of the school and the NPSD Central Office.

Technology Covered

NPSD may provide the privilege or Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, email, and more. The AUP applies to both District-owned technology equipment utilizing the NPSD network, the NPSD Internet connection, and/or private networks/Internet connections accessed from District-owned devices at any

time. Thus the AUP also applies to privately-owned devices accessing the NPSD network, the NPSD Internet connection, and/or private networks/Internet connections while on school property or participating in school functions or events off campus. NPSD policies outlined in this document cover all available technologies now and in the future, not just those specifically listed or currently available.

Promethean Board Usage

The District has a policy that addresses Promethean board usage. The following is in addition to and does not replace the separate Promethean board usage policy.

- Do not tape paper of any kind to the surface of the board.
- Do not use anything sticky such as large Post-It's, tape, putty, etc. on the board.
- Do not write on the board with dry erase markers or allow students to write on the board with markers or pens. If your lamp blows, please use the dry erase board in your room or the large Post-It's on a wall to conduct lessons until your replacement lamp is ordered and installed.
- Do not leave boards on if it will be inactive for more than 10 minutes.

Failure to comply with the guidelines of using the Promethean Board will result in the following:

1st Offense: Verbal Warning with documentation submitted to the Technology Department.

2nd Offense: Write-up to Building Administrator with documentation submitted to the Technology Department.

3rd Offense: Report submitted from the Technology Department to Central office to be placed in personnel file and based on damage(s) incurred; monetary retribution may be deducted from pay.

Network Security

Users are expected to take reasonable safeguards against the transmission of security threats over the NPSD network. This includes not opening or distributing infected files, programs, emails, or email attachments and not opening or accessing links, files, programs, emails, or email attachments of unknown or untrusted origin. Users should never share personal information, including student personal information. If users believe a computer or laptop they are using might be infected with a virus or other malicious code or program, they should immediately alert the Technology Department. Users should not attempt to remove the virus or malicious code themselves or download any programs to help remove the virus or malicious code.

Online Etiquette

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.

Users should recognize that among the valuable content online there is also unverified, incorrect, or inappropriate content. Users should only use known or trusted sources when conducting research via the Internet.

Users should remember not to post anything online (including but not limited to social media sites and services) that they would not want students, parents, teachers, or future colleges or employers to see. Once something is online, it cannot be completely retracted and can sometimes be shared and spread in ways the user never intended.

Plagiarism

Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they did not create themselves, or misrepresent themselves as an author or creator of something found online.

Information obtained via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission. This applies to both the personal information and the personal information of other users. Users should recognize that communicating over the Internet brings anonymity and associated risks and should carefully safeguard the personal information of themselves and others. Users should never agree to meet someone in person they meet online without parental permission. If users see a message, comment, image, or anything else online that makes them concerned for their personal safety or the safety of someone else, they should immediately bring it to the attention of an adult (teacher or administrator if at school, parent if the student is at home).

Cyber Bullying

Cyber bullying includes, but is not limited to, harassing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking will not be tolerated. Users should not send emails or messages, post comments, or take any other action online with the intent to harass, ridicule, humiliate, or harm the targeted individual and create for the targeted individual a hostile school environment.

Engaging in these behaviors or in any online activities intended to harm (physically or emotionally) another person, will result in disciplinary action. In some cases, cyber bullying can be a crime. Users should remember that online activities might be monitored.

Users will report to a staff member any attempt to cyber bully any other user or persons. NPSD will incorporate procedures to educate users about cyber bullying and take appropriate steps if a user has committed or is the victim of cyber bullying by another user. All students will be educated about appropriate online behavior.

Intentional, Malicious, and Willful Destruction of NPSD Devices

In the event a student intentionally, maliciously, and/or willfully damages or destroys any devices owned, leased, rented, provided by, or used by or in the NPSD, the student, student's parents, and/or guardians shall be required to reimburse NPSD for the full and complete cost of such damages. NPSD may pursue reimbursement and recovery for such damages, including but not limited to filing suit. NPSD may seek recovery of necessary court costs in the event it files suit to recover such reimbursement and recovery.

Social Media

The District has a policy that addresses Social Media, which applies to all employees and students. By signing the AUP, users are acknowledging they have read and agreed to abide by the Social Media guidelines.

Disclaimer of Liability

Internet use is a privilege, not a right. NPSD makes no warranties of any kind, either expressed or implied, for the access being provided.

- The staff, the school, and the NPSD are not responsible for any damages incurred, including, but not limited to, loss of data resulting from delays or interruption of service, for the loss of data stored on NPSD resources, or for personal property used to access NPSD resources.
- The NPSD will not be responsible for the accuracy, nature, or quality of information stored on NPSD resources or gathered through district provided access.
- The NPSD will not be responsible for unauthorized financial obligations resulting from use of district-provided access.
- Further, even though the NPSD may use technical or manual means to regulate access and information, these methods do not provide a foolproof means for enforcing the provisions of this policy. Therefore, NPSD will not be responsible for any damages incurred from technology resource access and/or failure to enforce this policy.
- NPSD reserves the right to amend and/or change this policy in whole or in part at any time. Notice will be given of any changes during the current school year.

Requirements

- Each user allowed access to NPSD technology resources must sign and date a contract agreeing to abide and enforce this policy on an annual basis and put on file with the Office of Superintendent.
- Student contracts must be signed and dated by the student, their parent or legal guardian, and their homeroom teacher annually and turned into the Office of Superintendent to be placed on file before access can be granted.
- Employee contracts must be signed and dated by the employee and their supervisor annually and turned into Central Office to be placed in their employee folder before access can be granted.
- Guest accounts can be provided on a case-by-case, time-limited basis. All guest accounts must sign and date an AUP contract and be reviewed by the Technology Coordinator and/or Network Administrator, before access can be granted.
- No users will be allowed access to NPSD technology resources without a signed and dated contract on file.

NORTH PANOLA SCHOOL DISTRICT

Technology Department

Dear Parent(s),

Please sign and remove the following sheets giving permission for your child to use the technology resources provided by the North Panola School District. These sheets should be returned to your child's homeroom teacher immediately. These forms will be picked from your child's schools and file by the Technology Department as part of the Child Internet Protection Act (CIPA) compliance.

If these permission sheet(s) are not returned, your child will not be allowed to use the technology resources of the North Panola School District [Reference the Children's Online Privacy Protection Act (COPPA) and the Children's Internet Protection ACT (CIPA)].

Thank you for your prompt attention in this matter,

Educationally Yours,

NPSD Technology Department