Section VI. TECHNOLOGY

NORTH PANOLA SCHOOL DISTRICT

Staff and Student Responsible Use Policy (RUP)

Original: August 2018; Revised: June 2019, September 2020, July 2021, June 2022

North Panola School District ("District") recognizes that access to technology at school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping our students develop global technology and communication skills. To facilitate this we provide access to various technologies for student and staff use.

This Responsible Use Policy ("Policy") outlines the guidelines and behaviors that all users are expected to follow when using District technology resources.

- The North Panola School District network is intended solely for educational purposes
- All activity over the network or using District resources may be monitored and retained
- Access to online content via the network will be restricted in accordance with our policies and applicable federal regulations, such as the Children's Internet Protection Act ("CIPA")
- Users are expected to follow the same rules for good behavior and respectful conduct online as offline
- Misuse of technology resources may result in disciplinary action
- North Panola School District makes a reasonable effort to ensure our users' safety and security online but will not be held liable for any harm or damages that result from the use of District technology resources
- Users of the District network or other technology resources are expected to alert Information Technology Services staff immediately of any concerns for safety or security

Responsible Uses of Technology (not all inclusive)

I will:

- Use District technologies for instructional activities
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- Treat District resources and equipment 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 staff member if I see threatening, inappropriate, or harmful content (images, messages, posts, or videos) online.
- Use District technologies at appropriate times, in approved places, and only for educational purposes.
- Cite sources when using online sites and resources for research.
- Recognize that the use of District technologies is a privilege and treat it as such.
- Be cautious to protect the safety of others and myself.
- Only communicate with students via District owned or approved communication platforms.
- Help protect the security of the District resources.

Non-Responsible Uses of Technology (not all inclusive)

I will not:

- Use District technologies in a way that could be harmful.
- Attempt to find inappropriate images or content, or attempt to circumvent the District's filtering tools.
- Engage in cyber bullying, harassment, or disrespectful conduct towards others.
- Plagiarize the content I find online.
- Share personally identifying information, about others or myself.
- Use District technologies for personal gain, product advertisement, political lobbying, or partisan political activities.
- Use language online that would be unacceptable in the classroom.
- Use District technologies for illegal activities or to pursue information on such activities.
- Attempt to hack or access sites, servers, or content that is not intended for my use.

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

Technology Covered

The District may provide technological resources for students, employees, contractors, guests or other parties to use including, but not limited to, Internet access, computers and/or computing devices (including related peripherals), videoconferencing capabilities, online collaboration capabilities, message boards, social networking, and email. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

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

Mobile Devices: The District may provide users with mobile computers or other devices to promote learning outside of the classroom or to support administrative and clerical needs. Users are expected to abide by the same responsible use policies when using devices off the District network as on the District network. Use of these devices while off the District network may be monitored.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the District is entrusting to your care. Users should report any loss, damage, or malfunction to Information Technology Services staff immediately. Users may be financially accountable for any damage resulting from negligence or intentional misuse.

Screen Care: Mobile devices and computer screens can be damaged if subjected to rough treatment or inappropriate usage. The screens of mobile devices are particularly sensitive to damage from excessive pressure on the screen.

- Do not lean on the top of mobile devices when they are closed.
- Do not place anything near the device when it is closed.
- Do not poke the screen.
- Do not place anything on the keyboard before closing the lid (i.e. pens, pencils, or disks).
- Do not bump the devices against walls, floors, etc. as it will eventually break the screen.
- Do not carry the device by the screen!

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 District, 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.

Usage Policies

As a condition of maintaining the privilege of using District computer resources, each user will be held responsible for his or her own actions which affect such resources. Each user acknowledges and agrees to abide by the terms of the Policy. A user who violates the Policy will be subject to appropriate discipline.

District technology resources are intended to be used for instruction, learning, District-related business, and administrative activities.

Internet Access & Use

The District provides its users with access to the Internet, including web sites, resources, content, and online tools. This access will be restricted in compliance with CIPA regulations and District policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Users shall comply with the access and security procedures and systems established to ensure the security, integrity and operational functionality of District network and computer resources.

Users shall not attempt to circumvent established protections and restrictions to download or attempt to download or run executable programs over the District network or onto District resources without express permission from Information Technology Services staff.

You may, however, be able to download other file types, such as images or videos. To ensure the security of the network download such files only from reputable sites, and only for educational purposes. Transmitting, receiving, or downloading of any material in violation of any U.S. or State regulations is prohibited. This prohibition includes, but is not limited to, copyrighted material, pornography, threatening or obscene material or images inappropriate to an instructional environment.

Personal Safety

Users should never share personal information including phone numbers, addresses, social security numbers, birthdates, or financial information over the Internet or via email. Communicating over the Internet brings anonymity and other associated risks and users should always carefully safeguard the personal information of themselves and others. Students should never agree to meet someone they have communicated with online in real life 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 using the device at home).

If you see a message, comment, image, video or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.

Accounts

Email: The District many provide users with email (or other communications platform) accounts, for the purpose of school-related communication. Availability and use may be restricted based on District policies.

If users are provided with email (or other communications platform) accounts, they should be used with care. Email (or other communications platform) is not a secure transmission protocol; messages are sent in clear text and may be intercepted. Users should never send personal information or attempt to open files or follow links from unknown or untrusted origins. Users shall refrain from profanity and vulgarity. Only communicate with other people as allowed by District policies or the teacher.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email (or other communications platform) usage may be monitored or archived.

Network: Accounts issued to users for the use of District technology resources are for the intended user's sole use only. Users are expected to keep login information private at all times and are responsible for any misuse that occurs under the accounts issued to them. They shall use the system only under their own accounts and shall maintain the privacy or personal information and passwords.

Students Under the Age of 13: For students under the age of 13, the Children's Online Privacy Protection Act (COPPA) requires parental permission for educational software tools. Parents who wish to deny their child(ren) access to these tools must do so in writing to the building administrator indicating that their child should not have access to the tools. Examples of these tools are Google Apps for Education and/or similar educational programs. Denying use of educational tools does not include state or district assessments.

Social Media: The school district, schools, and select organizations have social media accounts/pages that are monitored and maintained by the Public Relations Department and school/department administrators/designees. These social media outlets are meant to be a place for current students, parents, alumni, staff, and other district stakeholders to received information as it relates to awards, events, recognitions, ecetera for both employees and students of the District.

Fraternization via social media between District employees and current District students is prohibited. Student access to social media, like Facebook, Instagram or any other sites of a similar status, on any NPSD campus is prohibited.

In addition to this policy, the District has a policy that addresses Social Media (**Policy GABBA: Social Media Websites**), 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 in both policies.

Communication with Students

All communication with students shall be conducted on District owned or approved communications platforms. At no time shall any staff member, contractor, guest or other approved party use their personal accounts or any non-District approved communication platform to communicate with students.

Cyber Bullying

Cyber bullying includes, but is not limited to, harassing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking. It 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.

Data Security

District staff and students may have access to confidential and/or personally identifiable information ("PII") of students or staff. This information may not be shared with unauthorized third parties, and under no circumstances may it be transmitted electronically without the use of appropriate encryption and the prior approval of the Custodian of Records and or the Director of Technology. Confidential and/or personally identifiable information may not be stored on mobile computing devices or portable storage devices without encryption and the prior approval of the Custodian of Records and/or Director of Technology, and may not be transmitted via email under any circumstances.

Personal Equipment

The District recognizes that the use of certain technology devices which are not owned by the District may be beneficial District employees. District employees may connect personal laptops, tablets, or other computing devices to District wireless networks specified by the District, and do so at their own risk and agree to hold the District harmless. Personal equipment may not be connected to any other wired or wireless network owned by the District without express permission by the Director of Technology.

Security

Security on any computer system is of the highest priority. Users who identify a security problem must immediately notify a representative from Information Technology Services or an administrator. Users must never use any other user's accounts or share passwords with anyone, or leave account/password information where it may be discovered. Students may only use teacher computing equipment under the direct supervision of the teacher, and solely for instructional purposes. Any user identified as a security risk may be denied access to the system.

Users shall not attempt to "crash" or "hack" into District systems. Users shall not tamper with any software protections or restrictions placed on computer applications or files. Unless authorized to do so, users shall not attempt to access or modify restricted portions of any operating system, security software, system or network.

Users shall not attempt to remove existing software or add their own, personal software to District computers and systems unless authorized to do so. Any user who is authorized to install software or make systems changes on a particular device do so at their own risk and agree to hold the District harmless.

Netiquette

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

Users are expected to recognize that among the vast array of valuable content online there also exists unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.

Users should also remember not to post anything online that they wouldn't want parents, teachers, future colleges or potential employers to see. Once something is online, it is out of your control and can sometimes be shared and spread in ways you never envisioned or 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.

No Expectation of Privacy

District network, technology resources and all user accounts are the property of District. There is no right to privacy in the use of the network, technology resources or user accounts.

In addition, users are hereby put on notice as to the lack of privacy afforded by electronic data storage and electronic mail in general, and must apply appropriate security to protect private and confidential information from unintended disclosure. Electronic data, including email, which is transmitted through District technology resources, is more analogous to an open postcard than to a letter in a sealed envelope. Under such conditions, the transfer of information which is intended to be confidential should not be sent through District technology resources.

The District reserves the right to monitor and access information transmitted over its network or contained on its computer resources under various circumstances including, but not limited to, the following circumstances:

Under Mississippi Public Records Act ("MPRA"), electronic files are treated in the same way as paper files. Public documents are subject to inspection through MPRA. In responding to a request for information under the MPRA, District may access and provide such data without the knowledge or consent of the user.

The District may cooperate with any local, state, or federal officials investigating an alleged crime committed by any person who accesses District computer resources, and may release information to such officials without the knowledge or consent of the user.

The contents of electronic messages, including any email communication sent using District technological resources, may be viewed by Information Technology Services staff in the course of routine maintenance, or by the Director of Technology, or designee(s) as needed for District administrative purposes, including, but not limited to, investigation of possible violations of the Policy or other District policies, and monitoring of online activities of minor students.

Limitation of Liability

The District will not be responsible for damage or harm to persons, files, data, or hardware.

While the District employs, and makes reasonable efforts to ensure the proper functioning of filtering and other safety and security mechanisms, it makes no guarantees as to their effectiveness.

NPSD will not be responsible or liable for: financially or otherwise, unauthorized transactions conducted over the NPSD network.

Violations of this policy may have disciplinary consequences, including:

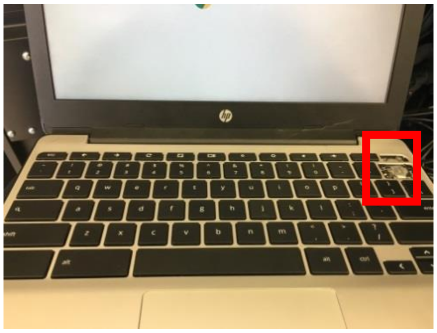
a. Suspension of network, technology, or computer privileges;
b. Notification of parents;
c. Detention or suspension from school and school-related activities;
d. Employment disciplinary action up to and including termination of employment; and/or,
e. Legal action and/or prosecution.

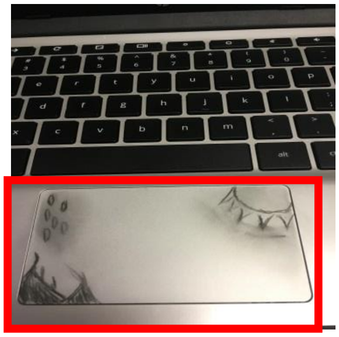
NPSD employees, students, and parents/guardians shall be required to sign the District's Acceptable Use Policy before Internet or network access shall be allowed. This policy applies to all devices and equipment purchases made through the Equity Distance Learning Act (EDLA) program for which the district assumes ownership and liability.

Violations of this Responsible Use Policy

Student Violations: Users shall report any suspected violation of the Policy by a student to a school site administrator, who shall immediately review the matter and take appropriate action including, if necessary, referring the matter to the Executive Director of Technology (or designee) for review. If the Executive Director of Technology (or designee) determines that a violation has occurred, the user may be subject to appropriate discipline, legal action, and/or prosecution.

Employee Violations: Users shall report any suspected violation of the Policy by a District employee to the employee's supervisor who shall immediately refer the matter to a Human Resources administrator for review. The Human Resources administrator (working in collaboration with the Executive Director of Technology or designee) shall then determine whether a violation of the Policy has occurred. If the Human Resources administrator determines that a violation has occurred, he or she may take immediate action (working in collaboration with the Executive Director of Technology or designee) to restrict, suspend, or revoke the user's privileges. The user may also be subject to appropriate discipline, legal action, and/or prosecution.





Cost of Repairs

Students will be held partially responsible for **ALL** damage to any device damage by their negligence and/or carelessness including but not limited to: broken screens, hinges, missing keys, etc. Mechanical failures will be covered by NPSD. All repair charges will be the sole responsibility of the student. A parent, guardian or custodian of a compulsory-school-age child enrolled in a public school district shall be responsible financially for his or her minor child's destructive acts against school property or persons [See Mississippi Code § 37-11-53(2)(a)]. Any public school district shall be entitled to recover damages in an amount not to exceed Twenty Thousand Dollars ($20,000.00), plus necessary court costs, from the parents of any minor under the age of eighteen (18) years and over the age of six (6) years, who maliciously and willfully damages or destroys property belong to such school district [See Mississippi Code § 37-11-53(4)].

Replacement costs are estimated as follows, but may be assessed in a higher amount depending on the type and extent of damage:

Device/Part	Cost
11-inch Chromebook	$190
14-inch Chromebook	$260
2020 Chromebooks	$348
Charger	$35 - $100
Computer	$800 or greater
Monitor	$200 (*Prices vary by size)
Keyboard	$30
Mouse	$10

Guidelines/Procedure Changes

The District reserves the right to change these guidelines / procedures at any time, without notice.

If you have any questions about any part of the RUP, including consequences or failure to comply with the RUP, please address your questions via email to Carla Malone, Director of Technology & Innovation at cmalone@northpanolaschools.org.

Acceptance of this Policy

All users agree to the stipulations set forth in the above document when the Agreement Form for the North Panola School District is signed.