REQUIRED **Descriptor Code: AC DA**

ACCEPTABLE USE

The Hettinger Public School District believes Internet access plays an important role in the education of students; however, the Internet also contains content that is not appropriate for students and staff to access. In accordance with federal law, the district has taken reasonable precautions to restrict access to materials obscene, pornographic, and/or harmful to minors through the use of software designed to block sites containing inappropriate material. While the District has taken such preventive measures, it recognizes that it *is* not possible to fully guarantee that students and/or staff will never access objectionable materials.

Education

The district shall provide education to students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

Monitoring Use

Internet access is a privilege, not a right. Network storage areas shall *be* subject to the same scrutiny as school lockers for students. Staff shall have no reasonable expectation of privacy when using district computers and/or networks and shall use this technology solely for work-related purposes. Technology Directors & Administrators may view files and communications to maintain the integrity of the system and to ensure proper and responsible use of the system. Teachers and administrators will exercise supervision of student use.

Software

Personal software will not be installed on school-owned computers or the network. To prevent computer viruses from being transmitted throughout the system, there will be no unauthorized downloading of any software without the technology director's consent.

Email

The e-mail system used in the Hettinger School Public District will only be Office365 K12 e-mail accounts.

Prohibitions
The Superintendent or designee may take disciplinary measures when any of the following actions occur:

1. Using obscene language.
2. Accessing or creating pornographic files or sites and/or other inappropriate material.
3. Harassing, insulting, threatening, alarming, or attacking others:
4. Vandalizing/Damaging computers, computer systems, or computer networks.
5. Violating copyright. trademark, trade secret, or other intellectual property laws.
6. Using or participating in chat rooms or social networking sites for personal and/or non-curricular purposes.
7. Using another's password or representing oneself as another.
8. Trespassing into another's account, folders, work, or files.
9. Intentionally wasting network resources including, but not limited to: emailing chain letters, cryptocurrency mining, hosting gaming servers and/or broadcasting inappropriate messages.
10. Employing the network for political purposes as defined by state law, financial gain, and/or commercial purposes.
11. Revealing anyone's personal information such as, but not limited to, an address or phone number without appropriate consent. Students are prohibited from revealing personal information about themselves and/or others without obtaining written consent in accordance with the Federal Education Rights and Privacy Act and receiving administrative approval.
12. Other activities or actions deemed inappropriate and not in the best interest of the district, its employees, and students.

Violations

Violation of this policy will, at a minimum, result in the following disciplinary consequences for students:

1. First offense (Level I)

   A. Loss of Office 365 (K12) email (Teams & OneDrive) at least 2 weeks
   B. Internet privileges for at least 2 weeks depending on admin decisions.
   C. Parents contacted.

2. Second offense (Level II)

A. Loss of Office 365 (K12) email (Teams & OneDrive) at least 4 weeks
B. Internet privileges for at least the remainder of the semester depending on admin decisions.
C. Parents contacted.

3. A student may be subject to Level II disciplinary action on his/her first offense if administration deems this necessary based on the severity of the offense.

Violations of this acceptable use policy or any applicable federal or state law rule, or regulation may also result in disciplinary action up to and including expulsion for students or termination of employment for staff

Consent

All students and staff must consent to this policy in writing (or digitally signed) prior to accessing district networks and/or computers.

Complimenting NED-SSA Templates (may contain items not adopted by the Board)

- FFK, Suspension & Expulsion
- FFK-BR, Suspension & Expulsion Regulations

End of Hettinger Public School District Policy ACD…….....…Adopted: June 15, 2015

Computer User Agreement Attachment 1

AI and LLM Policy

Educational Purpose:

Students must use AI tools solely for educational purposes as directed by teachers or school authorities. Using AI for non-educational activities or submitting AI work as original student work within the school context is prohibited.

Ethical Conduct:

Students are expected to use AI technologies ethically, respecting copyright laws, privacy norms, and the intellectual property rights of others. AI should not be used to engage in plagiarism, cheating, or any form of dishonesty in academic work. AI work must not be submitted in the place of student work.

Privacy and Data Protection:

Students must be cautious when interacting with AI tools that require personal information. Sharing sensitive or personal data without proper authorization or oversight is prohibited. Students should understand the risks and implications of data sharing and seek guidance from teachers when necessary.

Respectful Interaction:

Any form of communication with or through AI tools, including chatbots or virtual assistants, must adhere to the same standards of respect and decency expected in human interactions. Abusive, harmful, or disrespectful conduct through AI platforms is unacceptable.

Safety and Security:

Students must not use AI to access or disseminate harmful or inappropriate content. They should immediately report any security breaches, suspicious activities, or exposure to inappropriate content encountered during AI use to school authorities.

Resource Responsibility:

AI resources, such as software, chatbots, or assistants should be used responsibly and not abused for the ease of use in creating original content. Students should ensure that AI tools are used responsibly, without unnecessary ethical implications.

Monitoring and Compliance:

The school will monitor the use of AI technologies to ensure compliance with this policy. Monitoring will be conducted in an ethical manner, respecting the privacy and rights of students.

Violations of this policy may result in disciplinary action, including but not limited to, restriction of access to AI resources, educational interventions, or other disciplinary measures as deemed appropriate by the school administration.

- 1st Offense: Forfeiture of grade on assignments and a teacher conference.
- 2nd Offense: Forfeiture of grade on assignments and a parent/teacher conference.
- 3rd Offense: Forfeiture of grade on assignments and an administrator conference.
- All additional offenses will be handled by the administration.

Review and Update:

This policy will be reviewed and updated at any time to reflect new developments in AI technology, changes in legal and ethical standards, and the evolving needs of the educational environment.

Conclusion:

The responsible use of AI by students in the K-12 educational setting is essential for fostering a safe, ethical, and productive learning environment. By adhering to this policy, students will be better equipped to leverage AI technologies for their educational advancement while respecting the norms and values of our school community.