Hartland Consolidated Schools
Staff Acceptable Use Policy

Hartland Consolidated Schools (HCS) offers staff access to a computer network for educational and instructional purposes. In addition, HCS offers staff access to the Internet. Internet access is intended to promote, enhance, and support educational goals and objectives. All staff must sign the Acceptable Use Policy. A copy of the signed AUP will be stored electronically on a server.

District Network Security

Each staff member is provided with a network account, which allows access to network services and the Internet. This access is provided for those who agree to act in a considerate and responsible manner. Access is a privilege, not a right. Network accounts provide for a limited amount of personal storage space on the HCS network for files related to the pursuit of education, which must be maintained by periodically clearing out older files.

Computers and Servers are protected against viruses by software and virus updates are constantly monitored by Technology Staff to ensure they are current.

Staff computers will be kept secure by any end-user who uses them. When computer devices are left unattended, closing doors and keeping them locked as well as locking screens is required. Servers are kept in a locked room with minimal physical access. Only those who need access to the server rooms are allowed access.

HCS utilizes Internet filtering and Firewalls to help protect any district user from inappropriate material and bad actors intending to gain access to the network. Filtering is effective but not perfect. Staff must be vigilant in monitoring student use of technology systems and prepared to enforce the guidelines found within this policy (AUP). It is the expectation that ALL staff monitor students who are using Internet resources.

Individuals requesting unfiltered requests to the Internet must make that request to the Director of Technology and will be decided upon by a committee consisting of the Director of Technology, Principal, Assistant Superintendent of Curriculum and Instruction, Assistant Superintendent of Personnel and Student Services, and Superintendent.

Hartland Schools employs an extensive back-up of data each night. Copies are stored both on-site and off-site for additional security. For details, see the Disaster Recovery Plan.

Individual users of the district computer networks are responsible for their behavior and communications over those networks. Users will only use their personal user ID to log in to the HCS network. When signing the AUP users agree to comply with district rules and policies.

HCS makes no warranties of any kind, either expressed or implied, for the provided access. The staff, school and HCS are not responsible for any damages incurred, including, but not limited to, the loss of data stored on HCS resources, to personal property used to access HCS resources, or for the accuracy,

nature or quality of information stored on HCS resources. In the event of an electronic breach of data or disaster to the Network Server Room, the district will enact its Disaster Recovery Plan, outlined in the District Technology Plan.

No Expectation of Privacy; Monitoring

All usage of any Information System, and any electronic data created, sent, received or stored in the system are, and remain the property of, Hartland Consolidated Schools. The District treats ALL electronic data sent, received, or stored over its Information Systems as its business information. As a result, the District has the right to and will periodically assess whether specific Staff Users are using the District's Information Systems for authorized purposes. Because the Information Systems and all electronic data generated by it and stored in it are the property of the District, Staff Users should understand the they have NO expectation of privacy in their access and use of the District's Information Systems.

To safeguard and protect the District's proprietary, confidential, and business-sensitive information, and to ensure that the use of the District's Information Systems is consistent with the District's educational purposes, the District reserves the right to monitor the use of its Information Systems. This may include the monitoring of a Staff User's computer or Internet usage, printing and/or reading of e-mail, listening to voice-mail messages, and viewing of any other electronic data on its Information Systems. Accordingly, the District reserves the right to monitor and log each Staff User's computer and Internet usage to maximize e-mail and fileserver space utilization.

Hardware and Software Disposal

It can be dangerous to continue to use equipment or software that is not capable of being kept up to date and doing so can open the district to cyber attacks. Technology at Hartland Consolidated Schools is used through the end of its useful life. Once the Technology Department has deemed hardware or software has reached the end of its useful life, that equipment will be disposed of in a manner that is environmentally responsible and secure.

Passwords; User Responsibilities

All pass codes, passwords; ID.'s and encrypted information are the property of the Hartland Consolidated Schools. No Staff User may use a pass code, password, I.D. or method of encryption that has not been issued specifically to that Staff User by Hartland Consolidated Schools. In other words, no Staff User may give, even on a temporary basis, his or her pass code, password, or I.D. to another Staff User or Student without prior written approval by the District. Every Staff User is responsible for, and should take all reasonable precautions to protect, his or her pass-code, password, and I.D.
Each Staff User is advised that transferring files, shareware, and other software can transmit computer viruses and should exercise extreme care and caution in doing so.

Social Media Use

An employee's personal or private use of social media may have unintended consequences. While the Board respects its employees' First Amendment rights, those rights do not include permission to post inflammatory comments that could compromise the District's mission, undermine staff relationships, or

cause a substantial disruption to the school environment. This warning includes staff members' online conduct that occurs off school property, including from the employee's private computer. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

Use of Artificial Intelligence/Natural Language Processing Tools

The use of AI in district programs or operations must be in accordance with 7540.04.

Staff are permitted to use Artificial Intelligence and Natural Language Processing (NLP) tools (collectively, "AI/NLP tools") to accomplish their job responsibilities so long as the use is ethical, responsible, and does not violate any provisions of this policy (e.g., it does not infringe on students' or staff members' privacy rights, violate their duty to maintain confidentiality related to personally identifiable information, etc.).

With respect to students, it is the Board's policy that they are required to rely on their own knowledge, skills, and resources when completing school work. In order to ensure the integrity of the educational process and to promote fair and equal opportunities for all students, except as outlined below, students are prohibited from using AI/NLP tools to complete schoolwork. The use of AI/NLP tools without the express permission/consent of a teacher is considered to undermine the learning and problem-solving skills that are essential to a student's academic success and that the staff is tasked to develop in each student. Consequently, students are encouraged to develop their own knowledge, skills, and understanding of course material rather than relying solely on AI/NLP tools, and they are expected to ask their teachers when they have questions and/or need assistance. A student's unauthorized use of AI/NLP tools is considered a form of plagiarism and any student found using such tools without permission or in a prohibited manner will be disciplined in accordance with the Student Code Of Conduct.

Notwithstanding the preceding, students are allowed to use AI/NLP tools in the school setting if they receive prior permission/consent from their teacher, so long as they use the AI/NLP tools in an ethical and responsible manner. Teachers Have the discretion to authorize students to use AI/NLP tools for the following uses:

A. Research assistance: AI/NLP tools can be used to help students quickly and efficiently search for and find relevant information for their school projects and assignments.
B. Data Analysis: AI/NLP tools can be used to help students to analyze, understand, and interpret large amounts of data, such as text documents or social media posts. This can be particularly useful for research projects or data analysis assignments – e.g., scientific experiments and marketing research.
C. Language translation: AI/NLP tools can be used to translate texts or documents into different languages, which can be helpful for students who are learning a new language or for students who are studying texts written in a different language.
D. Writing assistance: AI/NLP tools can provide grammar and spelling corrections, as well as suggest alternative word choices and sentence structure, to help students improve their writing skills.
E. Accessibility: AI/NLP tools can be used to help students with disabilities access and understand written materials.For example, text-to-speech software can help students with specific learning disabilities or visual impairments to read texts and AI-powered translation tools can help students with hearing impairments to understand spoken language.

As outlined above, under appropriate circumstances, AI/NLP tools can be effectively used as a

supplement to and not are placement for traditional learning methods. Consequently, with prior teacher permission/consent, students can useAI/NLP tools to help them better understand and analyze information and/or access course materials. If a student has any questions about whether they are permitted to use AI/NLP tools for a specific class assignment, they should ask their teacher.

Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked and disciplinary action taken against them. Users are personally responsible and liable, both civilly and criminally, for uses ofDistrict Information & Technology Resources that are not authorized by this policy and its accompanying guidelines.

The Board designates the Superintendent and Director of Technology as the administrators responsible for initiating,implementing, and enforcing this policy and its accompanying guidelines as they apply to staff member use of DistrictInformation & Technology Resources.

In addition, Federal and State confidentiality laws forbid schools and their employees from using or disclosing student education records without parental consent. See Policy 8330. Education records include a wide variety of information;posting personally identifiable information about students is not permitted. Staff members who violate State and Federal Confidentiality and/or privacy laws related to the disclosure of student or employee personally identifiable information may be disciplined.

Restrictions

The following activities are not permitted on the HCS electronic resources:

- Accessing, uploading, downloading, transmitting, displaying or distributing obscene or sexually explicit material.
- Accessing, uploading, downloading, transmitting, displaying, or distributing unauthorized files or applications of any kind (including but not limited to games, and Internet Proxies).
- Transmitting obscene, abusive or sexually explicit language.
- Damaging or vandalizing computers, computer systems, computer networks or computer files.
- Debilitating, disabling or altering computers, systems or networks.
- Creating, downloading, or distributing computer viruses or malware.
- Violating copyright or otherwise using another person’s intellectual property without his or her prior approval and/or proper citation.
- Using another person’s account, password, folder, work or files.
- Intentionally wasting computer network or printer resources.
- Using the HCS network or equipment for commercial or political purposes.
- Using the HCS network or equipment for personal purposes in such a way as to violate any other aspect of the Acceptable Use Policy. Or using the HCS network or equipment for personal purposes in such a way that causes a disruption in the ability of the employee to carry out his/her assigned responsibilities.
- Violating local, state or federal statutes.

Consequences for Improper Use

Inappropriate use of the HCS network will result in the restriction or suspension of the user's account.

Violations of the AUP may lead to disciplinary and/or legal action, including but not limited to termination or criminal prosecution by government authorities.

User Agreement

As a user of the Hartland Consolidated Schools computer network, I agree to comply with the Acceptable Use Policy (AUP). I will use the HCS network and the Internet in a constructive and appropriate manner. Should I commit any violation, my access privileges may be revoked, and disciplinary action will be taken.

User (print): _____

User Signature: _____

Staff Position: _____

Date: _____