Student Acceptable Use Policy

Hartland Consolidated Schools

Technology directly affects the ways in which information is accessed, communicated, and transferred in society. Educators are expected to continually adapt their means and methods of instruction, and the ways they approach student learning, to incorporate the latest technologies. The Board of Education provides Information & Technology Resources to support the educational and professional needs of its students and staff. With respect to students, District Information & Technology Resources afford them the opportunity to acquire the skills and knowledge to learn effectively and live productively in a digital world. The Board provides students with access to the Internet for educational purposes only and utilizes online educational services/apps to enhance the instruction delivered to its students. The District's computer network and Internet system does not serve as a public access service or public forum, and the Board imposes reasonable restrictions on its use consistent with its stated educational purpose.

The Board regulates the use of District Information & Technology Resources in a manner consistent with applicable local, State, and Federal laws, the District's educational mission, and articulated expectations of student conduct as delineated in the Student Code of Conduct. Board Policy and the Student Code of Conduct govern students' use of District Information & Technology Resources and students' personal communication devices when they are connected to District Information & Technology Resources, including online educational services/apps, regardless of whether such use takes place on or off school property.

Students are prohibited from using District Information & Technology Resources to engage in illegal conduct (e.g., libel,slander, vandalism, harassment, theft, plagiarism, inappropriate access, etc.) or conduct that violates this Policy and its related administrative guidelines and the Student Code of Conduct (e.g., making personal attacks or injurious comments,invading a person's privacy, etc.). Nothing herein, however, shall infringe on students' First Amendment rights. Because itsInformation & Technology Resources are not unlimited, the Board may institute restrictions aimed at preserving these resources, such as placing limits on the use of bandwidth, storage space, and printers.

Students have no right or expectation to privacy when using District Information & Technology Resources (including, but not limited to, privacy in the content of their personal files, messages/emails, and records of their online activity).

While the Board uses various technologies to limit students using its Information & Technology Resources to only use/access online educational services/apps and resources that have been pre-approved for the purpose of instruction,study, and research related to the curriculum, it is impossible to prevent students from accessing and/or coming in contact with online content that has not been pre-approved for use by students of certain ages. It is no longer possible for educators and community members to review and screen materials to assess their appropriateness for supporting and enriching the curriculum according to approved guidelines and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them)when significant portions of students' education take place online or through the use of online educational services/apps.

Pursuant to Federal law, the Board implements technology protection measures that protect against (e.g., filter or block)access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors,as defined by the Children's Internet Protection Act (CIPA). At the discretion of the Board or the Superintendent, the technology protection measures may be configured to protect against access to other material considered inappropriate for students to access. The Board also utilizes software and/or hardware to monitor online activity of students to restrict access to child pornography and other material that is obscene, objectionable, inappropriate, and/or harmful to minors. The Technology protection measures may not be disabled at any time that students may be using District Information & Technology Resources if such disabling will cease to protect against access to materials that are prohibited under the CIPA.Any student who attempts to disable the technology protection measures will be disciplined.

The Superintendent or Director of Technology may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material, if access to such sites has been mistakenly, improperly, inadvertently blocked by the technology protection measures. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measures.

Parents are advised that a determined user may be able to gain access to online content and/or services/apps that theBoard has not authorized for educational purposes. In fact, it is impossible to guarantee students will not gain access through the Internet to content that they and/or their parents may find inappropriate, offensive, objectionable, or controversial. Parents of minors are responsible for setting and conveying the standards that their children should follow when using the Internet.

Principals are responsible for providing training so that students under their supervision are knowledgeable about this policy and its accompanying guidelines.

Pursuant to Federal law, students shall receive education about the following:

A. safety and security while using e-mail, chat rooms, social media, and other forms of direct electronic communications;
B. the dangers inherent with the online disclosure of personally identifiable information;
C. the consequences of unauthorized access (e.g., "hacking"), cyberbullying, and other unlawful or inappropriate activities by students online;
D. unauthorized disclosure, use, and dissemination of personal information regarding minors

Staff members shall provide guidance and instruction to their students regarding the appropriate use of District Information & Technology Resources and online safety and security as specified above. Additionally, such training shall include, but not limited to, education concerning appropriate online behavior, including interacting with others on social media and in chat rooms and cyberbullying awareness and response. Furthermore, staff members will monitor the online activities of students while they are at school.
Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions, or use of specific monitoring tools to review browser history and network, server, and computer logs.

In order to keep District Information & Technology Resources operating in a safe, secure, efficient, effective, and beneficial manner to all users, students are required to comply with all District-established cybersecurity procedures including, but not limited to, the use of multi-factored authentication for which they have been trained. Principals are responsible for providing such training on a regular basis and measuring the effectiveness of the training.

Students will be assigned a District-provided school email account that they are required to utilize for all school-related electronic communications, including those to staff members, peers, individuals, and/or organizations outside the District With whom they are communicating for school-related projects and assignments. Further, as directed and authorized by their teachers, they shall use their school-assigned e-mail account when signing up/registering for access to various online educational services/apps.

Students are responsible for good behavior when using District Information & Technology Resources – i.e., behavior comparable to that expected of students when they are in physical classrooms and school buildings and at school-sponsored events. Because communications on the Internet are often public in nature, general school rules for behavior and communication apply. The Board does not approve any use of its Information & Technology Resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

Students may only use District Information & Technology Resources to access or use social media if it is done for educational purposes in accordance with their teacher's approved plan for such use.

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.

Hartland Consolidated Schools technologies have not been established as a public access or public forum and our school district has the right to place reasonable restrictions on the material you may access or post, the training you need to have before you are allowed to use the systems, and enforce all rules set forth in the Hartland School's code of conduct and the laws of the state of Michigan and the Federal U.S. Government. Further, you may not use these systems for commercial purposes to offer, provide, or purchase products or services through the systems or use them for political lobbying. Access to the Internet is available through the school district only with the permission of the Principal or his/her designee and your parent(s)/legal guardian. Hartland Consolidated schools is in compliance with the Child Internet Protection Act.

Students 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 school work. 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 a replacement for traditional learning methods. Consequently, with prior teacher permission/consent, students can use AI/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.

CIPA Compliance

The Hartland Consolidated Schools has and will continue to comply with the requirements of the Children's Internet Protection Act, as codified at 47 U.S.C. § 254(h) and (l). The district is committed to ensuring the safe conduct of all students while online and has a comprehensive policy about the proper use of our technological resources. At the beginning of each school year, students and staff are made aware of the district's Acceptable Use Policy. In addition, each student must sign an Internet use agreement before they are allowed access to the Internet both when they enter the district and each time they are promoted to a new building. It is the district's intent to preserve network bandwidth and improve network response times by limiting Internet access to educational-related sites. The district employs Internet content filtering software used to block and filter access to the Internet from pornographic and obscene sites, ensuring compliance with district policies and maintaining a positive environment.

The following are examples of acceptable uses and unacceptable uses of Hartland Consolidated School's technologies (which may include but are not limited to the following examples). This includes any technology equipment on or off District premises or at District events.

1. Personal Safety
    a. You will not post contact information (e.g., name, address, phone number…) about yourself or any other person.
    b. You will not agree to meet with someone you have met online without approval of your parents. Any contact of this nature or the receipt of any message you feel is inappropriate or makes you feel uncomfortable must be reported to your teacher or other district employee or technology team member.
2. Illegal/Prohibited Activities
    a. Students are prohibited from using District Information & Technology Resources to engage in illegal conduct or conduct that violates this policy. Nothing, however, shall infringe on students' First Amendment rights. Because its Information & Technology Resources are not unlimited, the Board may institute restrictions aimed at preserving these resources, such as placing limits on use of bandwidth, storage space, and printers.
    b. You will not attempt to gain unauthorized access to any District technology system, or individual equipment or go beyond your authorized access by entering another person's account or accessing another person's files.
    c. You will not deliberately attempt to disrupt/physically tamper with the computers, or network systems, or destroy data by spreading computer viruses (or malware) or by any other means.
    d. You will not use any technology equipment on District premises or at District events, or District equipment at any location to engage in any illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of a person, etc.
3. System Security
    a. You are responsible for your individual account and will take all reasonable precautions to prevent others from being able to use your account. Under no condition should you give your password to another person. Passwords to any electronic system should not be easily determined by others.
    b. You will immediately notify a teacher or the system Technology team if you have identified a possible security problem. Do not look for security problems: This will be considered an illegal attempt to gain access.
    c. You will avoid the inadvertent spread of computer viruses (or malware) by having all disks, downloads, or videos scanned for virus and malware.
    d. Each user of the technologies will ensure that all food and drink is kept away from all the equipment.
4. Integrity
    a. On any and all uses of technology equipment on District premises or at District events, or District equipment at any location whether in material posted on the Web, or internal documents, you will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language. You will not post information that could cause danger or disruption or engage in personal attacks, including prejudicial or discriminatory attacks.
    b. You will not use any technology equipment on District premises or at District events, or District equipment at any location to harass another person by any action that distresses or annoys. This includes developing software programs or publicly posting information that harasses others or might be considered cyberbullying.
5. Respect for Privacy
    a. Students have no right or expectation to privacy when using District Information & Technology Resources (including, but not limited to, privacy in the content of their personal lives, messages/emails, and records of their online activities.
    b. You will not repost communications or information that was sent to you privately without permission of the person who sent you the information.
    c. You will not post private information about yourself or another person.

6. Respecting Resource Limits
    a. You will use the system only for educational and career development activities and limited, high-quality, self-discovery activities. There is no limit on the use for education and career development activities. The limit on self-discovery activities will be defined by your supervising staff members.
    b. You will not load or download any executable (program) file or other large files without permission from a supervising staff member.
    c. Students shall not use a technology system or network to play games. Educationally based games shall be allowed under staff supervision.
    d. You are responsible for limiting use of disk space and deleting unnecessary files in a timely manner.
    e. Students shall not stream unauthorized video or music.
    f. Students will only use student wireless or guest wireless network to connect any personal electronic device to the Hartland Schools network. This includes but is not limited to laptops, computers, and any handheld electronic device. This access will be CIPA compliant, and will pass through the district's firewall and filter.
7. Electronic Communication
    a. Students will not access any chat room from any school district owned technology unless under the supervision of a teacher or administrator.
    b. Students will have limited use of district provided email accounts to facilitate learning and enhance the exchange of educational information. This use will be academic in nature only and will be monitored by the supervising staff member. - You will not post chain letters or engage in "spamming" (that is, sending an annoying or unnecessary message to a large number of people). - You will check your email frequently, delete unwanted messages promptly.
    c. Students may only use District Information & Technology Resources to access or use social media if it is done for educational purposes and in accordance with their teacher's approved plan for such use.
    d. You are responsible for maintaining the integrity of the e-mail system and reporting any violations of privacy or inappropriate behavior.
8. Plagiarism and Copyright Infringement
    a. You will not plagiarize works that you find on any of Hartland's technology systems, including the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours.
    b. You will respect the rights of copyright owners. Copyright infringement occurs when you inappropriately reproduce a work (including software, text, images etc.) that is protected by copyright. If a work contains language that specifies appropriate use of that work, you should follow the expressed requirements. If you are unsure whether or not you can use a work, you should request permission from the copyright owner, and cite references for all data accessed via technology. Direct any questions regarding copyright issues to a teacher or library media specialist.
9. Inappropriate Access to material
    a. You will not use Hartland technology systems to access material that is profane or obscene (pornography) or that advocates illegal acts or violence or discrimination toward other people (hate literature). A special exception may be made for hate literature if the purpose of the access is to conduct research with both teacher and parental approval.
    b. If you mistakenly access inappropriate information, you must immediately tell your teacher or other district employee or technology team member. This will protect you against a claim of intentional violation of this policy.
    c. Students/Parents/Guardians will be responsible for any financial expenses incurred by the district due to unauthorized use by a student. (i.e. on-line purchases)
    d. Your parents should instruct you if there is additional material they think would be inappropriate for you to access. The district fully expects that you will follow your parent's' instruction in this matter.
    e. Students shall not use a proxy to bypass our content filter.
    f. To the extent that any student uses non-district technology services to communicate information regarding the schools or its staff or students, Board policy still applies. This includes posting information, videos, or photos on services such as Facebook, YouTube, or any other social media site. Users and parents/guardians of students acknowledge that the district cannot control content posted to non-district technology services. Users and parents/guardians of students further acknowledge that the district

cannot filter non-district communication services such as cellular phone networks, nor control content stored on non-district equipment.

10. Your Rights
    a. Free Speech. Your right to free speech, as set forth in the school disciplinary code, applies also to your communications on the Internet. The Internet is considered a limited forum, similar to the school newspaper, and therefore the district may restrict your speech for valid educational reasons. The district will not restrict your speech on the basis of its disagreement with the opinions you express.
    b. Search and Seizure. You should expect no privacy of the contents of your personal files on the district's technology systems. Routine maintenance and monitoring of the system will occur and that monitoring could discover that you have violated this policy, the school code, or the law. An individual search will be conducted if there is reasonable suspicion that you have violated this policy, the Hartland Consolidated School's disciplinary code, or the law. The investigation will be reasonable and related to the suspected violation. Parents/legal guardians have the right at any time to see the contents of your files and directories.
    c. Due Process. The district will cooperate fully with local, state, or federal officials in any investigation related to illegal activities conducted through the Hartland Technology Systems. In the event of a claim that you have violated this policy, the Hartland Consolidated School's disciplinary code, or the law in your use of this system, you will be given notice of suspected violations and an opportunity to present an explanation according to school code and/or state and federal law. Additional restrictions may be placed on your use of Technology accounts.
    d. Use of Artificial Intelligence (AI)/Natural Language Processing Tools (NLP). Students 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, the use of artificial intelligence and natural language processing tools is strictly prohibited for the completion of school work. The use of AI/NLP tools without the express permission/consent of a teacher, undermines the learning and problem-solving skills that are essential to academic success. Unauthorized use of AI/NLP tools is considered a form of plagiarism and any student found using these tools without permission or in a prohibited manner will be disciplined in accordance with the Student Code of Conduct.
    e. Students may use AI/NLP tools in the school setting if they receive prior permission/consent from their teacher, so long as they use the tools in an ethical and responsible manner.

The district makes no guarantee that the functions or the services provided by or through the district system will be error-free or without defect. The district will not be responsible for any damage you may suffer including, but not limited to, loss of data or interruptions of service. The district is not responsible for the accuracy or quality of the information obtained through or stored on the system. The district will not be responsible for financial obligations arising from unauthorized use of the systems.

Parents are advised that a determined user may be able to gain access to online content and/or services/apps that the Board has not authorized for educational purposes. In fact, it is impossible to guarantee students will not gain access through the Internet to content that they and/or their parents may find appropriate, offensive, objectionable, or controversial. Parents of minors are responsible for setting and conveying the standards that their children should follow when using the Internet.

<u>Disciplinary Action</u>

When you are using the system, it may feel like you can more easily break a rule and not get caught. This is not true. Electronic footprints are imprinted on the system whenever an action is performed. Therefore, you are likely to be caught if you break the rules.

Any infraction involving the use of technology systems will be subject to consequences consistent with the Student Handbook and may include removal from computing systems or networks, detentions, suspensions of various duration, and/or recommendation to the Board for expulsion. **Loss of Internet or Network privileges may have a serious impact on a student’s grade and participation in technology related courses. Students may be required to use technologies off-campus to complete assignments outside of class. Students who lose network and/or Internet**

privileges due to a violation of the Acceptable Use Policy may be removed from a computer based class or have his/her schedule changed (resulting in loss of credit for the class) if loss of computer privileges will not allow for completion of class assignments, projects, and tests.

Physical tampering or destruction of technology will result in consequences based on the vandalism policy found in the student handbook. These consequences may include loss of technology access, which could result in loss of academic credit.

In addition, students/parent/guardian may be required to make full financial restitution to cover the loss of staff time and/or loss of equipment and/or any legal expense that may have been incurred during investigations of student misuse.

Photograph images of students in Grades PreK-12

Images and student work are permitted and may be used on district websites and social media. If parents wish to opt out of student image or student work publishing, it is necessary for them to properly fill out the “Parent Release Form” upon enrollment or re-enrollment in the Student Information System.

Student AUP Signature Form

I hereby release the Hartland Consolidated Schools' Technology systems and their operators and sponsors, Hartland Consolidated Schools and its faculty and staff and all organizations, groups and institutions with which the Hartland Consolidated Schools' Technology systems are affiliated for any and all claims of any nature arising from my use, or inability to use, the Hartland Consolidated Schools' Technology systems. I have read the entire policy, understand its content, and agree to abide by the terms and conditions therein. I further understand that any violation of the regulations above is prohibited and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, and disciplinary and/or appropriate legal action taken. My signature on this policy summary indicates I have read the terms and conditions carefully, understand their significance and agree to abide by them.

Parent or Legal Guardian Consent - As the parent or guardian of this student, I have read the Hartland Consolidated Schools Technology Acceptable Use Policy and Agreement. I understand that this access is designed for educational purposes. I recognize it is impossible for Hartland Consolidated Schools to restrict access to all controversial materials and I will not hold it responsible for materials acquired on the technology systems. I also understand that I will be responsible for any financial expenses incurred by the district due to unauthorized use by my child. I hereby give permission to issue a technology account in the indicated areas for my child and certify that the information contained on this form is correct.

My signature below indicates that I understand that my child will have access to computer devices and Internet content.

- Elementary students work on teacher supervised projects only.
- Academic email accounts intended for academic communications only are granted for all students fifth through twelfth grade.

As a user of the Hartland Consolidated Schools computer network, I agree to comply with the Acceptable Use Policy (AUP). I will use the Hartland Consolidated Schools' network and Internet resources in a constructive and appropriate manner intended for academic purposes. I understand that should I commit any violation, my computer access privileges may be revoked, and disciplinary action will be taken.

Student Name (Print): ____________________________________ Date: ____________________

Student Signature: ____

As a parent or legal guardian of the student above, I have read and understand the HCS Acceptable Use Policy.

Parent Name (Print): ____________________________________ Date: ____________________

Parent Signature: ____