Garaway Local Schools
Chromebook and Acceptable Use Policy

The policies, procedures, and information within this document apply to all Chromebooks used at Garaway Local Schools by students.

Teachers may set additional requirements for Chromebook use in their classroom.

Receiving Your Chromebook:

Chromebooks will be distributed each fall during the first week of school. ***Parents & Students must sign and return the Acceptable Use Policy Sign-off document before the Chromebook can be issued to their child.*** This document will need to be signed during student registration.

Insurance:

Garaway School suggests parents consider insurance to be purchased prior to deployment of the Chromebook to your child. Parents can self insure the devices through any private insurance if you choose.

Training:

Students will be trained on how to use the Chromebook by their homeroom teacher and other staff.

Return:

Student Chromebooks and accessories (carrying case, charger and battery) will be collected at the end of each school year for maintenance over summer vacation. Students will retain their original Chromebook each year while enrolled at Garaway High School and receive ownership of upon completion of 12th grade.

Any student who transfers out of Garaway School, before the end of the first year of the program, will be required to return their Chromebook and accessories. If a Chromebook and accessories is not returned, the parent/guardian will be held responsible for payment in full. If payment is not received the parent/guardian will be turned over to a collection agency.

If a student is going to attend Buckeye Career Center they will have the option to purchase the computer for the remaining portion of the technology fee.

Taking Care of Your Chromebook:

Students are responsible for the general care of the Chromebook which they have been issued by the school. Chromebooks that are broken or fail to work properly must be taken to the Assistant's Principal Office. The student will need to fill out a repair ticket. The technology department will notify the student when the computer is repaired.

General Precautions:

- No food or drink is allowed next to your Chromebook.
- Cords, cables, and removable storage devices must be inserted carefully into the Chromebook.
- Students should never carry their Chromebook while the screen is open unless directed to do so by a teacher.
- Chromebooks should be shut down when not in use to conserve battery life.
- Chromebooks should never be shoved into a locker or wedged into a book bag as this may break the screen.
- Do not expose your Chromebook to extreme temperature or direct sunlight for extended periods of time. Extreme heat or cold may cause damage to the laptop.
- Always bring your laptop to room temperature prior to turning it on.

Carrying the Chromebook:

The "always on" case for the Chromebook will only provide basic protection from everyday use. It is not designed to prevent damage from drops or abusive handling. Carrying the Chromebook in it's case is mandatory at all times. For example, you shouldn't toss the case or drop the case while your Chromebook is inside. Keep your name tag on the case at all times.

Screen Care:

The Chromebook screen can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure on the screen.

- Do not lean on top of the Chromebook.
- Do not place anything near the Chromebook that could put pressure on the screen.
- Do not place anything in the carrying case that will press against the cover.
- Do not poke the screen.
- Do not place anything on the keyboard before closing the lid (e.g. pens, pencils, notebooks).
- Clean the screen with a soft, dry anti-static, or micro-fiber cloth. Do not use window cleaner or any type of liquid or water on the Chromebook. You can also purchase individually packaged pre-moistened eyeglass lens cleaning tissues to clean the screen. These are very convenient and relatively inexpensive.

Using Your Chromebook

At School:
The Chromebook is intended for use at school each and every day. In addition to teacher expectations for Chromebook use, school messages, announcements, calendars, academic handbooks, student handbooks and schedules will be accessed using the Chromebook. Students must be responsible for bringing their Chromebook to all classes, unless specifically advised not to do so by their teacher.

Email:

- Students in need of email for academic reasons will only be allowed email access through an address assigned by the district. This email access will be through a Google Gmail system managed by Garaway. The interface is heavily monitored by corporation network administrators and is subject to filtering of inappropriate content.
- Always use appropriate language.
- Do not transmit language/material that is profane, obscene, abusive, or offensive to others.
- No private chatting during class without permission is allowed.
- Email is subject to inspection at any time by school administration.
- Students will only be able to communicate with other Garaway students and faculty.

At Home:
Parents are fully responsible for the devices off school property. All students are required to take their Chromebook home each night throughout the school year for charging. ***Chromebooks must be brought to school each day in a fully charged condition.*** Students need to charge their Chromebooks each evening. If students leave their Chromebook at home, they must immediately phone parents to bring the Chromebook to school. Repeat violations of this policy will result in referral to administration and possible disciplinary action.

Sound:
Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.

Printing:

At School: Printing functionality will be available on a limited basis at school and subject to classroom requirements.

At Home: The Chromebook will not support a physical printer connection. Instead, users may print to their home printers using the Google Cloud Print service. A wireless home network is required for this. http://google.com/cloudprint

Managing Your Files and Saving Your Work:

Students may save documents to their Google Drive, or they may save to an external memory device such as a miniSD card or USB flash drive. Saving to Google Drive will make the file accessible from any computer with internet access. Students using Google Drive to work on their documents will not need to save their work, as Drive will save each keystroke as the work is being completed. It will be the responsibility of the student to maintain the integrity of their files and keep proper backups. Students will be trained on proper file management procedures.

Personalizing the Chromebook:

Chromebooks must remain free of any decorative writing, drawing, stickers, paint, tape, or labels that are not the property of Garaway School. Spot checks for compliance will be done by administration or Garaway School Technicians at any time.

Software on Chromebooks:

Originally Installed Software:
Chromebook software is delivered via the Chrome Web Store. These are web-based applications that do not require installation space on a hard drive. Some applications, such as Google Drive, are available for offline use. The software originally installed on the Chromebook must remain on the Chromebook in usable condition and easily accessible at all times.

All Chromebooks are supplied with the latest build of Google Chrome Operating System (OS), and many other applications useful in an educational environment. The Chrome OS will automatically install updates when the computer is shutdown and restarted.

From time to time the school may add software applications for use in a particular course. This process will be automatic with virtually no impact on students. Applications that are no longer needed will automatically be removed by the school as well.

Virus Protection:
Virus protection is unnecessary on the Chromebook due to the unique nature of its design.

Additional Software:
Students are unable to install additional software on their Chromebook other than what has been approved by Garaway School.

Inspection:
Students may be selected at random to provide their Chromebook for inspection. The purpose for inspection will be to check for proper care and maintenance as well as inappropriate material being carried into the school.

Procedure for Restoring the Chrome OS:
If technical difficulties occur, technical support staff will use the "5-minute" rule. If the problem cannot be fixed in 5 minutes, the Chromebook will be restored to factory defaults. In a One-to-One environment it is impossible for support staff to maintain a working environment for all if too much time is spent fixing every glitch that may arise. Restoring the Chrome OS will restore the device to the state in which the user originally received it. All student created files stored on an external miniSD card, USB flash drive, or Google Drive will be intact after the operating system is restored. All files saved on the chromebook that have been synced to Google Drive will be intact.

Protecting & Storing Your Chromebook:

Chromebook Identification:
Chromebooks will be labeled in the manner specified by the school.
Chromebooks can be identified in the following ways:

- Record of serial number and Garaway asset tag
- Individual's name

Under no circumstances are students to modify, remove, or destroy identification labels.

Storing Your Chromebook:
When students are not monitoring their Chromebook, they should be stored in their lockers *with the lock securely fastened.* Nothing should be placed on top of the Chromebook, when stored in the locker. Students need to take their Chromebook home with them every night. The Chromebook is not to be stored in their lockers or anywhere else at school outside of school hours. The Chromebook should be charged fully each night at the student's home. Chromebooks should *never* be stored in a vehicle.

Storing Chromebooks at Extra-Curricular Events:
Students are responsible for securely storing their Chromebook during extra-curricular events.

Chromebooks Left in Unsupervised / Unsecured Areas:
Under no circumstance should a Chromebook be stored in unsupervised areas. Unsupervised areas include the school grounds, the cafeteria, unlocked classrooms, library, locker rooms, dressing rooms, hallways, bathrooms, extra-curricular bus, in a car, or any other entity that is not securely locked or in which there is not supervision.

Unsupervised Chromebooks will be confiscated by staff and taken to the Assistant Principal's office. Disciplinary action will be taken for leaving a Chromebook in an unsupervised location.

Repairing or Replacing Your Chromebook:

Chromebooks Undergoing Repair:

- Loaner Chromebooks may be issued to students when they leave their Chromebook for repair.
- If repair is needed due to malicious damage, the school may refuse to provide a loaner Chromebook.
- Repaired Chromebooks will end up with the original factory image as first received. It is important that students keep their school data synced to cloud drives so documents and class projects will not be lost.
- Students and parents will be charged for Chromebook damage that is a result of misuse or abusive handling. Parents will be billed for parts and labor.

Manufacturer Warranty:

Samsung warrants the Chromebook from defects in materials and workmanship for a period of one year. This warranty is only valid for the first 12 months from the date Garaway School takes delivery of the Chromebook. This limited warranty covers normal use, mechanical breakdown, or faulty construction and will provide replacement parts necessary to repair or if necessary, replace the Chromebook. The Samsung warranty ***DOES NOT*** warrant against damage caused by misuse, abuse, or accidents. Please report all Chromebook problems at the Assistant Principal's Office.

If a Chromebook becomes defective (at no fault of the student) after the Samsung warranty expires, Garaway School will replace the Chromebook at no charge with a refurbished Chromebook of the same age or newer.

Accidental Damage or Loss Protection:

As part of the 1:1 Chromebook initiative at Garaway School, the school is offering the purchase of accidental damage insurance prior to the deployment of the Chromebook to your child. The family of the student will be the sole provider of this insurance. Under this insurance policy the Chromebooks are protected against accidental damage or loss due to an act of nature. The school will require that a police report be submitted in cases of theft. Fraudulent reporting of theft will be turned over to the police for prosecution. A student making a false report will also be subject to disciplinary action.

This insurance policy does not cover for loss of the Chromebook and/or its accessories, cosmetic damage, or damages caused by intentional misuse and abuse. Garaway School will assess the Chromebook damage and repair or replace the device if the damage is determined to be accidental and within the protection guidelines. **Parents/Students will be charged for full replacement cost of a device that has been damaged due to intentional misuse or abuse.**

Lost or Intentionally Damaged Device and Accessories:
A Chromebook or any of it's accessories that are lost (whereabouts unknown) or intentionally damaged is the responsibility of the student and parent involved in the loss of property. The user will not be given another device or accessory to use until the replacement cost of the lost/damaged device or accessory is paid to the school.

- Replacement of the Chromebook $220
- AC Adapter & power cord - $20
- "Always on" Case - $30
- Screen $35.00

Book	Policy Manual
Section	7000 Property
Title	STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY
Code	po7540.03
Status	Active
Adopted	December 12, 2011
Last Revised	May 15, 2023

7540.03 - **STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY**

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 way they approach student learning to incorporate the latest technologies. The Board of Education provides Information & Technology Resources (as defined in Bylaw 0100) (collectively, "District 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 do not serve as a public access service or a 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. This policy and its related administrative guidelines 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 (see Policy 5136).

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 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.

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/e-mails, 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 adopted 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 the 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 CIPA. Any student who attempts to disable the technology protection measures will be disciplined.

The Superintendent or Technology Director 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, or 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 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 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", "harvesting", "digital piracy", "data mining", etc.), cyberbullying, and other unlawful or inappropriate activities by students online; and

D. unauthorized disclosure, use, and dissemination of personally-identifiable 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 be limited to, education concerning appropriate online behavior including interacting with others on social media, including 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.

All students who use District Information & Technology Resources (and their parents if they are minors) are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines. See Form 7540.03 F1.

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.

Use of Artificial Intelligence/Natural Language Processing Tools For School Work

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 (AI) and Natural Language Processing (NLP) tools (collectively, "AI/NLP 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 and that the staff is tasked to develop in each student. Students are encouraged to develop their own knowledge, skills, and understanding of course material rather than relying solely on AI/NLP tools and they should ask their teachers when they have questions and/or need assistance. 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.

Notwithstanding the preceding, students can 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 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 such resources 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 of District Information & Technology Resources that are not authorized by this policy and its accompanying guidelines.

The Board designates the Superintendent and Technology Director as the administrator(s) responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to students' use of District Information & Technology Resources.

Revised 11/19/12
Revised 12/8/14
Revised 11/20/17

Legal P.L. 106-554, Children's Internet Protection Act of 2000

18 U.S.C. 1460

18 U.S.C. 2246

18 U.S.C. 2256

20 U.S.C. 6777, 9134 (2003)

20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)

47 C.F.R. 54.500 - 54.523

47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)

Book	Administrative Guideline Manual
Section	7000 Property
Title	STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY
Code	ag7540.03
Status	Active
Adopted	November 1, 2012
Last Revised	May 15, 2023

7540.03 - **STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY**

Students shall use District Information & Technology Resources (see definition Bylaw 0100) for educational purposes only. District Information & Technology Resources shall not be used for personal, non-school related purposes. Use of District Information & Technology Resources is a privilege, not a right. When using District Information & Technology Resources, students must conduct themselves in a responsible, efficient, ethical, and legal manner. Students who engage in unauthorized or inappropriate use of District Information & Technology Resources, including any violation of these guidelines, may have their privilege limited or revoked, and may face further disciplinary action consistent with the Student Code of Conduct/Student Handbook and/or civil or criminal liability. Prior to accessing or using District Information & Technology Resources, students (eighteen (18) years of age and older) and parents of minor students must sign the Student Technology Acceptable Use and Safety Agreement (Form 7540.03 F1). Parents should discuss their values with their children and encourage students to make decisions regarding their use of District Information & Technology Resources that are in accord with their personal and family values, in addition to the Board's standards.

This guideline also governs students' use of personally-owned communication devices (PCDs) (see definition Bylaw 0100) when the PCDs are connected to District Information & Technology Resources or when used while the student is on Board-owned property or at a Board-sponsored activity.

Below is a non-exhaustive list of unauthorized uses and prohibited behaviors. This guideline further provides a general overview of the responsibilities users assume when using District Information & Technology Resources.

A. All use of District Information & Technology Resources must be consistent with the educational mission and goals of the District.

B. Students may only access and use District Information & Technology Resources by using their assigned account. Use of another person's account/e-mail address is prohibited. Students may not allow other users to utilize their account/e-mail address and should not share their password or other multifactor authentication (MFA) device/app with other users. Students may not go beyond their authorized access. Students should take steps to prevent unauthorized access to their accounts by logging off or "locking" their PCDs when leaving them unattended and employing MFA techniques whenever possible/available.

C. No user may access another person's private files. Any attempt by users to access another user's or the District's non-public files, or phone or e-mail messages, is prohibited. Any attempts to gain access to unauthorized resources or data/information on District Information & Technology Resources or other services/apps are prohibited. Similarly, students may not intentionally seek information on, obtain copies of, or modify files, data, or passwords belonging to other users, or misrepresent other users on the District's Information & Technology Resources.

D. Students may not intentionally disable any security features used on District Information & Technology Resources.

E. Students may not use District Information & Technology Resources or their PCDs to engage in vandalism, "hacking," or other illegal activities (e.g., software pirating; intellectual property violations; engaging in slander, libel, or harassment; threatening the life or safety of another; stalking; transmission of obscene materials or child pornography, including sexting; fraud; or sale of illegal substances and goods).

1. Slander and Libel - In short, slander is "oral communication of false statements injurious to a person's reputation," and libel is "a false publication in writing, printing, or typewriting or in signs or pictures that maliciously damages a person's reputation or the act or an instance of presenting such a statement to the public." (The American Heritage Dictionary of the English Language. Third Edition is licensed from Houghton Mifflin Company. Copyright © 1992 by Houghton Mifflin Company. All rights reserved.) Students shall not knowingly or recklessly post/publish false or defamatory information about a person or organization. Students are reminded that material distributed over the Internet is "public" to a degree no other school publication or utterance is. As such, any remark may be seen by literally millions of people, and harmful and false statements will be viewed in that light.

2. Students shall not use District Information & Technology Resources to transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, national origin, sex (including sexual orientation or gender identity), age, disability, religion, or political beliefs. Sending, sharing, viewing, or possessing pictures, text messages, e-mails, or other materials of a sexual nature (e.g., sexting) in electronic or any other form, including the contents of a PCD or other electronic equipment, is grounds for discipline. Such actions will be reported to local law enforcement and child services as required by law.

3. Vandalism and Hacking – Deliberate attempts to damage the hardware, software, or information residing in District Information & Technology Resources or any services/apps attached through the Internet are strictly prohibited. In particular, malicious use of District Information & Technology Resources to develop programs that harass other users or infiltrate District Information & Technology Resources or PCDs and/or damage District Information & Technology Resources or PCDs is prohibited.

   Attempts to violate the integrity of private accounts, files, programs, or services/apps, the deliberate infecting of District Information & Technology Resources or PCDs attached to the network with a "virus", and/or attempts at hacking into any internal or external computer systems using any method will not be tolerated.

   Students may not engage in vandalism or use District Information & Technology Resources or their PCDs in such a way that would disrupt others' use of District Information & Technology Resources.

   Vandalism is defined as any malicious or intentional attempt to harm, steal, or destroy data/information of another user or District Information & Technology Resources. This includes, but is not limited to, creating and/or uploading computer viruses, installing unapproved software, changing equipment configurations, deliberately destroying or stealing hardware and its components, or seeking to circumvent or bypass network security and/or the Board's technology protection measures. Students also must avoid intentionally wasting limited resources. Students must immediately notify a teacher, or Principal if they identify a possible security problem. Students should not go looking for security problems, because this may be construed as an unlawful attempt to gain access.

4. Students shall not use District Information & Technology Resources to access, process, distribute, display, or print prohibited material at any time, for any purpose. Students may only access, process, distribute, display, or print restricted material and/or limited access material as authorized below.

   a. Prohibited material includes material that constitutes child pornography and material that is obscene, objectionable, inappropriate, and/or harmful to minors, as defined by the Children's Internet Protection Act (CIPA). As such, the following material is prohibited: material that appeals to a prurient or unhealthy interest in nudity, sex, and excretion; material that depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and material that lacks serious literary, artistic, political, or scientific value as to minors. Prohibited material also includes material that appeals to a prurient or unhealthy interest in, or depicts, describes, or represents in a patently offensive way, violence, death, or bodily functions; material designated as for "adults" only; and material that promotes or advocates illegal activities.

   b. Restricted material may not be accessed by elementary or middle school students at any time, for any purpose. Restricted material may be accessed by high school students in the context of specific learning activities that have been approved by a teacher or staff member for legitimate research

purposes. Materials that may arguably fall within the description provided for prohibited material that has clear educational relevance, such as material with literary, artistic, political, or scientific value, will be considered to be restricted. In addition, restricted material includes materials that promote or advocate the use of alcohol and tobacco, hate and discrimination, satanic and cult group membership, school cheating, and weapons. Sites that contain personal advertisements or facilitate making online connections with other people are restricted unless such sites have been specifically approved by the Building Principal.

c. Limited access material is material that is generally considered to be non-educational or entertainment. Limited access material may be accessed in the context of specific learning activities that are directed by a teacher or during periods that a school may designate as "open access" time. Limited access material includes such material as electronic commerce, games, jokes, recreation, entertainment, sports, and investment.

If a student inadvertently accesses material that is considered prohibited or restricted, the student should immediately disclose the inadvertent access to the teacher or Principal. This will protect the student against an allegation that the student intentionally violated the provision.

The determination of whether material is prohibited, restricted, or limited access shall be based on the content of the material and the intended use of the material, not on the protective actions of the technology protection measures. The fact that the technology protection measures have not protected against access to certain material shall not create the presumption that such material is appropriate for students to access. The fact that the technology protection measures have blocked access to certain material shall not create the presumption that the material is inappropriate for students to access.

5. Unauthorized Use of Software or Other Intellectual Property from Any Source – All communications and information accessible via the Internet should be assumed to be private property (i.e., copyrighted and/or trademarked). Laws and ethics require proper handling of intellectual property. All copyright issues regarding software, information, and attributions/acknowledgment of authorship must be respected.

   Software is intellectual property and, with the exception of freeware, is illegal to use without legitimate license or permission from its creator or licensor. All software loaded on District Information & Technology Resources must be approved by the Technology Director, and the District must own or otherwise obtain, maintain, and retain the licenses for all copyrighted software loaded on District computers. Students are prohibited from using District Information & Technology Resources for the purpose of illegally copying another person's software. Illegal peer-to-peer file trafficking of copyrighted works is prohibited.

   Online articles, blog posts, podcasts, videos, and wiki entries are also intellectual property. Students should treat information found electronically in the same way they treat information found in printed sources – i.e., properly citing sources of information and refraining from plagiarism. Rules against plagiarism will be enforced.

F. Transmission of any material in violation of any State or Federal law or regulation, or Board policy, is prohibited.

G. Students may not use District Information & Technology Resources for private gain or commercial purposes (e.g., purchasing or offering for sale personal products or services by students), advertising, or political lobbying.

H. Students may not use District Information & Technology Resources to engage in cyberbullying. "Cyberbullying" involves the use of information and communication technologies to support deliberate, repeated, and hostile behavior by an individual or group, which is intended to harm others. (Bill Belsey (http//www.cyberbullying.org)) Cyberbullying may occur through e-mail, instant messaging (IM), chat room/Bash Boards, small text messages (SMS), websites, voting booths, social media, and other technological means of communicating/publishing text, audios, and/or videos.

   Cyberbullying includes, but is not limited to, the following:

   1. posting/publishing slurs or rumors or other disparaging remarks about a student on a website or weblog;

   2. sending e-mails or instant messages that are mean or threatening or so numerous as to negatively impact the victim's use of that method of communication and/or drive up the victim's cell phone bill;

   3. using a smartphone to take and/or send embarrassing and/or sexually explicit photographs/recordings of students;

4. posting/publishing online misleading or fake photographs of students.

I. Students are expected to abide by the following generally-accepted rules of online etiquette:

1. Be polite, courteous, and respectful in your messages to others. Use language appropriate to school situations in any communications made through or utilizing District Information & Technology Resources. Do not use obscene, profane, lewd, vulgar, rude, inflammatory, sexually explicit, defamatory, threatening, abusive, or disrespectful language in communications made through or utilizing District Information & Technology Resources.

2. Do not engage in personal attacks, including prejudicial or discriminatory attacks.

3. Do not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a student is told by a person to stop sending that person messages, the student must stop.

4. Do not post information that, if acted upon, could cause damage or a danger of disruption.

5. Never reveal names, addresses, phone numbers, or passwords of yourself or other students, family members, teachers, administrators, or other staff members while communicating on the Internet. This prohibition includes, but is not limited to, disclosing personally identifiable information on commercial websites.

6. Do not transmit to third parties/unknown individuals pictures or other information that could be used to establish identity without prior approval of a teacher.

7. Never agree to get together with someone you "meet" online without parent approval and participation.

8. Regularly check District-provided e-mail account and delete e-mails no longer need.

9. Students should promptly disclose to a teacher or administrator any messages they receive that are inappropriate or make them feel uncomfortable, especially any e-mail that contains sexually explicit content (e.g. pornography). To aid in any investigation, students should not delete such messages until instructed to do so by an administrator.

J. Downloading of files onto District Information & Technology Resources is prohibited without prior approval from the principal. If a student transfers files from online services/apps (e.g., electronic bulletin board services), the student must check the file with a virus detection program before opening the file for use. Only public domain software may be downloaded. If a student transfers a file or installs a program that infects District Information & Technology Resources with a virus and causes damage, the student will be liable for any and all repair costs associated with making the District Information & Technology Resources once again fully operational.

K. Students must secure prior approval from a teacher before joining a Listserv (electronic mailing lists) and should not post personal messages on bulletin boards or Listservs.

L. Students may use real-time electronic communication, such as chat or instant messaging, only under the direct supervision of a teacher or in moderated environments that have been established to support educational activities and have been approved by the Board, Superintendent, or Principal. Students may only use their school-assigned accounts/e-mail addresses when accessing, using, or participating in real-time electronic communications for education purposes.

M. Users have no right or expectation to privacy when using District Information & Technology Resources. The Board reserves the right to access and inspect any facet of District Information & Technology Resources including, but not limited to, computers, laptops, tablets, and other web-enabled devices, networks, or Internet connections or online educational services or apps, e-mail or other messaging or communication systems, or any other electronic media within the District's technology systems or that otherwise constitutes its property and any data, information, e-mail, communication, transmission, upload, download, message, or material of any nature or medium that may be contained therein. A student's use of District Information & Technology Resources constitutes the student's waiver of any right to privacy in anything the student creates, stores, sends, transmits, uploads, downloads, or receives on or through District Information & Technology Resources and related storage medium and equipment. Routine maintenance and monitoring, utilizing both technology monitoring systems and staff monitoring, may lead to discovery that a user has violated Board policy/guidelines and/or the law. An individual search will be conducted if there is reasonable suspicion that a user has violated Board policy and/or law, or if requested by local, State, or Federal law enforcement officials. Students' parents have the right to request to see the contents of their children's

files, e-mails, and records.

The following notice will be included as part of the computer log-on screen:

"District Information & Technology Resources (as defined in Bylaw 0100) are to be used for educational and professional purposes only. Users are reminded that all use of District Information & Technology Resources, including Internet use, is monitored by the District and individual users have no expectation of privacy."

N. Use of the Internet and any data/information procured from the Internet is at the student's own risk. The Board makes no warranties of any kind, either express or implied, that the functions or services provided by or through District Information & Technology Resources will be error-free or without defect. The Board is not responsible for any damage a user may suffer including, but not limited to, loss of data/information, service interruptions, or exposure to inappropriate material or people. The Board is not responsible for the accuracy or quality of data/information obtained through the Internet. Data/Information (including text, graphics, audio, video, etc.) from Internet sources used in student papers, reports, and projects must be cited the same as references to printed materials. The Board is not to be responsible for financial obligations arising through the unauthorized use of District Information & Technology Resources. Students or parents of students will indemnify and hold the Board harmless from any losses sustained as the result of a student's misuse of District Information & Technology Resources.

O. Disclosure, use, and/or dissemination of personally identifiable information of minors via the Internet is prohibited, except as expressly authorized by the minor student's parent/guardian on the "Student Technology Acceptable Use and Safety Agreement Form" (see Form 7540.03 F1).

P. Proprietary rights in the design of websites, web pages, and services/apps hosted on Board-owned or District-affiliated servers remain at all times with the Board.

Q. File-sharing is strictly prohibited. Students are prohibited from downloading and/or installing file-sharing software or programs on District Information & Technology Resources.

R. Since there is no central authority on the Internet, each site is responsible for its own users. Complaints received from other sites regarding any of the District's users will be fully investigated and disciplinary action will be imposed as appropriate.

S. Preservation of Resources and Priorities of Use: District Information & Technology Resources are limited. Each student is permitted reasonable space to store e-mail, web, and personal school-related files. The Board reserves the right to require the purging of files in order to regain space on data storage devices. Students who require access to District Technology Resources for class- or instruction-related activities have priority over other users. Students not using District Information & Technology Resources for class-related activities may be "bumped" by any student requiring access for a class- or instruction-related purpose.

T. **Artificial Intelligence/Natural Language Processing Tools**: Absent express direction/permission from a teacher, a student may not use Artificial Intelligence (AI) or Natural Language Processing (NLP) tools to complete school work – i.e., to create, compose, generate, or edit original content that they intend to submit as their own work. This prohibition includes, but is not limited to, the use of AI and NLP tools to prepare a writing assignment or creative art project or to answer questions on a quiz, test, or in-class or homework assignment. The preceding prohibition does not include and does not limit a student’s use of AI/NLP tools that are features built into apps, including a word processing program, installed by the District on District-issued PCDs (e.g., Chromebooks), or AI/NLP tools that is/are listed as approved accommodation(s) or assistive technology pursuant to a student’s individualized education program or Section 504 Plan. In particular, this prohibition does not include the use of speech-to-text features that are part of District-issued PCDs unless the purpose of the class work/assignment is to assess/test a student’s knowledge of spelling, grammar, etc. If a student has any question(s) as to whether specific AI/NLP tools can be used for an assignment, the student should ask their teacher. If a student violates this prohibition, the student will be charged with plagiarism and disciplined in accordance with the Student Code of Conduct, including not receiving credit for the assignment.

Abuse of Network Resources

Peer-to-peer file sharing, mass mailings, and downloading of unauthorized games, videos, and music are wasteful of limited network resources and forbidden. In addition, the unauthorized acquisition and sharing of copyrighted materials are illegal and unethical.

Unauthorized Printing

District printers may only be used to print school-related documents and assignments. Printers, like other school resources, are to be used in a responsible manner. Ink cartridges and paper, along with printer repairs and replacement, are very expensive. The District monitors printing by users. Print jobs deemed excessive and abusive of this privilege may result in charges being assessed to the student. Users are prohibited from replacing ink cartridges and performing any other service or repairs to printers. Users should ask, as appropriate, for assistance to clear paper that is jamming a printer.

Any questions and concerns regarding these guidelines may be directed to the IT Department.

Legal

P.L. 106-554, Children's Internet Protection Act of 2000

20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)

18 U.S.C. 1460

18 U.S.C. 2246

18 U.S.C. 2256

20 U.S.C. 6777, 9134 (2003)

47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)

Garaway Local Schools

146 Dover Road NW, Sugarcreek, Ohio 44681 (330) 852-2421 x2

Dr. James A. Millet, Superintendent · Sheryl Hardesty, Treasurer

STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY AGREEMENT

To access and use District Information and Technology Resources (as defined in Bylaw 0100) (collectively, "IT Resources"), including a school-assigned email account and/or the Internet at school, students under the age of eighteen (18) must obtain parent/guardian permission and sign and return this form. Students eighteen (18) and over may sign their own forms.

Use of District IT Resources is a privilege, not a right. The Board of Education's IT Resources, including its computer network, Internet connection, and online educational apps/services, are provided for educational purposes only. Unauthorized and inappropriate use will result in loss of this privilege and/or other disciplinary action. Students who sign this Agreement are affirming that they will not use District IT Resources for illegal, unethical, or harassing purposes or to access online content that may be considered obscene, pornographic, or unsuitable for children.

The Board has implemented technology protection measures that protect against (e.g., block/filter) Internet access to visual displays/depictions/materials that are obscene, constitute child pornography, or are harmful to minors. The Board also monitors online activity of students in an effort to restrict access to child pornography and other material that is obscene, objectionable, inappropriate, and/or harmful to minors. Nevertheless, parents/guardians are advised that determined users may be able to gain access to information, communication, and/or services on the Internet that the Board has not authorized for educational purposes and/or that they and/or their parents/guardians may find inappropriate, offensive, objectionable or controversial. Students using District IT Resources are personally responsible and liable, both civilly and criminally, for unauthorized or inappropriate use of such resources.

The Board has the right, at any time, to access, monitor, review, and inspect any directories, files, and/or messages received by, residing on, or sent using District IT Resources. Messages relating to or in support of illegal activities will be reported to the appropriate authorities. Individual users have no expectation of privacy related to their use of District IT Resources.

Policy and Administrative Guideline 7540.03 can be found at www.garaway.org/FormsDownloads.aspx. Scroll down to Student Related Forms.

Please complete the following information:

Student User's Full Name (please print): _____

School:_____ Grade: _____

School Year: _____

Parent/Guardian's Name: _____

Parent/Guardian

As the parent/guardian of this student, I have read Policy and Administrative Guideline 7540.03 - Student Technology Acceptable Use and Safety, and discussed them with my child. I understand that student access to the Internet is designed for educational purposes and that the Board has taken available precautions to restrict and/or control student access to material on the Internet that is obscene, objectionable, inappropriate, and/or harmful to minors. However, I recognize that it is impossible for the Board to restrict access to all objectionable and/or controversial materials that may be found on the Internet. I will not hold the Board (or any of its members, officers, employees, or administrators) responsible for content my child may come in contact with while on the Internet. Additionally, I accept responsibility for communicating to my child the standards (i.e., family values) I want them to follow when using the Internet, including how they should go about selecting, sharing, and exploring information and resources on the Internet. I further understand that individuals and families may be liable for violations of the Policy and Guidelines.

If my child, as part of a class assignment, designs and/or develops a website, web page, or app/service that is hosted on Board-owned or District-affiliated servers, I agree the Board shall be entitled to retain proprietary rights in the website, web page, or app/service such that the Board shall have a license in perpetuity to use the website, web page, or app/service without any compensation or remuneration to me or my child.

By signing this form I agree to the following:

- I give permission for the Board to issue an email account to my child.
- I give permission for my child's image (photograph) to be published online, provided only their first name is used.
- I give permission for the Board to transmit "live" images of my child (as part of a group) over the Internet via a web cam.
- I authorize and license the Board to post my child's class work on the Internet without infringing upon any copyright my child may own with respect to such class work. I understand only my child's first name will accompany such class work.

Parent/Guardian's Signature: _____ Date: _____

Student

I have read and agree to abide by Policy and Administrative Guideline 7540.03 - Student Technology Acceptable Use and Safety. I understand that any violation of the terms and conditions set forth in the Policy and Guidelines may result in disciplinary action and/or referral to law enforcement. As a user of District IT Resources, I agree to communicate over the Internet and through the IT Resources in an appropriate manner, honoring all relevant laws, restrictions, and guidelines.

Students who are eighteen (18) years of age or older need to initial the following:

If, as part of a class assignment, I design and/or develop a website, web page, or app/service that is hosted on Board-owned or District-affiliated servers, I agree the Board shall be entitled to retain proprietary rights in the website, web page, or app/service such that the Board shall have a license in perpetuity to use the website, web page, or app/service without any compensation or remuneration to me.

Student's Signature: _____ Date: _____

Teachers and building principals are responsible for determining what is unauthorized or inappropriate use. The Principal may deny, revoke, or suspend access to and use of the District IT Resources to individuals who violate the Board's Student Technology Acceptable Use and Safety Policy and related Guidelines, and take such other disciplinary action as is appropriate pursuant to the Student Code of Conduct.