

Willoughby-Eastlake City Schools Chromebook Handbook



“Preparing graduates to meet the challenges of the 21st century.”

Introduction

Providing students with the technology tools necessary to support instructional goals and effective operations is a priority for the Willoughby-Eastlake City School District. With this goal in mind, we are pleased to implement our 1:1 Chromebook initiative.

Parent/Guardians/Student Chromebook Agreement

The Google Chromebook and any accessories are the property of the Willoughby-Eastlake City School District. The Chromebooks on loan to the students must be used in accordance with the following agreement and procedures, District policies, as well as those outlined in the Technology Acceptable Use Policy (AUP) for Students. Appropriate and responsible use is expected of all users. Violation of any policies or procedures outlined in the Technology Acceptable Use Policy or the Chromebook Handbook will be subject to the appropriate disciplinary action as outlined in the AUP and the student code of conduct.

Receiving a Chromebook

Students in Grades 3-12 will be assigned a Chromebook, case and a charger to bring back and forth from home to school. Students in Grades K-2 will be assigned a Chromebook from a dedicated classroom Chromebook cart for use throughout the school day. Parents/guardians of students in Grades K-2 may request for their Chromebook to be utilized at home through arrangements with the building administration and classroom teacher.

Returning a Chromebook

Students in Grades 4-7 and 9-11 will keep their Chromebooks over the summer and are expected to bring them to school on the first day of the following school year. Students in Grades 3, 8 and 12 will return their Chromebooks for maintenance and redistribution over the summer. Parents/guardians of students in summer school or District sponsored enrichment programs in Grades 3 and 8 may request a device to use over the summer by emailing helpdesk@weschools.org. Students who unenroll from the District for any reason must immediately return their Chromebook.

Technology Fee

An annual technology fee of \$20 will be required for all students to defray the cost of technology and associated digital software related to student learning. Payment of the annual technology fee by the last day of the first quarter, will cover the cost of one repair as a result of accidental damage during the school year. If multiple repairs are needed from one incident, the highest value repair will be covered. Full device replacement or lost chargers are not covered by the annual technology fee. The annual fee will be assessed August 1st and will cover the school year through July 31st. *Families who do not typically pay school fees due to free and reduced lunch status, may choose to pay the technology fee to receive the benefit of the covered repair cost outlined above.* Payment of the technology fee is non-refundable.

Ownership

The Willoughby-Eastlake City School District retains the sole right of ownership and possession of the Chromebook. These Chromebooks are lent exclusively to the students of the Willoughby-Eastlake City Schools and should not be used by anyone other than the student it was assigned to. Each Chromebook is assigned to an individual student. Students should never "swap" or "share" their Chromebook with another student, friend, or sibling. The administrative staff and faculty retain the right to collect and/or inspect Chromebooks at any time, to monitor student work or to update, add or delete installed software or hardware.

** Students who attend the School of Innovation in the graduating classes of 2027, 2028 and 2029 will be offered the opportunity to pay the previously agreed \$50 annual fee. Once the fees, totaling \$200, have been collected, the ownership will be transferred to the family at the completion of 8th grade. Affected families who would like to have the benefit of having the first annual repair covered, may also pay the \$20 annual Technology Fee in addition to the previously agreed \$50 annual fee.*

Web-filtering

The Willoughby-Eastlake City School District does not have control over information found on the Internet. Our District uses the content filter, "Lightspeed" to keep students safe on their school-issued devices. This program allows us to comply with CIPA (Children's Internet Protect Act) regulations and monitor all internet activity on the school-issued Chromebooks on school property and while the device is off of school grounds. Using a content filter helps to keep our students safe on-line and is a requirement for federal funding. Content filters make every attempt to block access to inappropriate content but parents/guardians will still need to monitor and supervise the information their students are accessing from the Internet while off campus. Parents/guardians are responsible for student use of the Internet outside of the District. It is the responsibility of the parent/guardian to monitor student's Chromebook use at home.

Privacy

Network, internet, and access to a device is provided as an educational tool. The District has the right to randomly inspect any Chromebook, application, or peripheral device. This includes but is not limited to browser history, email, media that has been accessed, downloaded or created, documents, pictures, and all files. The District has the right to review these items for appropriateness and to limit or revoke a student's access to them.

Classroom Use

Use of the computer for anything other than teacher directed or approved activities during instructional time is prohibited. This includes, but is not limited to, internet or computer games and other entertainment activities, email, instant messaging, chat, and use of the Internet for anything other than school-related research. Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes. Earbuds/headphones may be used based upon individual teacher approval.

Devices Left at Home

Students who leave their Chromebooks at home are responsible for completing their coursework as if they had their Chromebook present. A student who repeatedly leaves their Chromebook at home will be subject to appropriate disciplinary action.

Use and Care of Devices

- Devices assigned to students in grades 3-12 must always be kept in their school assigned Chromebook case.
- Students are not permitted to add marking, etching, or stickers to the devices or cases, nor remove serial numbers or asset tags.
- Students will bring their devices to school fully charged.
- Only use a soft, lint-free microfiber cloth to clean the screen. Do not use window cleaner or any other household cleaner to clean the device or screen.
- Avoid getting moisture or liquids on the device/accessories.
- Devices must never be left in an unsupervised, unlocked or unsecured space on or off of school grounds.
- Do not consume food or drink on or near the device.
- Avoid placing anything on top of the device. Too much pressure will crack the screen.
- Avoid cramming a device in a locker or bag.
- Extreme heat or cold can harm the device.
- Do not leave a device where it can be stepped or sat on. It may cause significant damage.
- Pornographic, obscene, or vulgar images, sounds, music, language or materials, including screen savers, backgrounds, and or pictures are prohibited. District policy will be followed. Students will not use the Chromebook for illegal purposes.
- Students will not deliberately use the Chromebook to personally attack, annoy, harass, or bully others. Any such activities will be reported to the appropriate District personnel as well as local, state, or federal authorities.
- Do not disassemble or attempt to repair your device. All repairs must be made by the Willoughby-Eastlake City Schools Technology Department.

Repairs

All repairs must be completed by the Willoughby-Eastlake City Schools Technology Department. When a device needs repaired the student must bring the device to the building's designated repair processing area. If the Chromebook cannot be fixed at that time, a loaner device will be issued. All device policy agreements will remain in effect for the loaner or other assigned device. If you are in need of a repair over the summer please email helpdesk@weschools.org to request an appointment.

Repair Fines

Parents/guardians are responsible for the cost of repairs that are required as a result of accidental damage, intentional damage, neglect, and/or vandalism as determined by the Willoughby-Eastlake City Schools Technology Department. Payment of the annual technology fee by the last day of the first quarter will cover the cost of one repair as a result of malfunction or accidental damage during the school year. All other repairs will be charged based on the following fine schedule. Some repairs may require multiple parts.

Repair Type	Cost
Entire Device Replacement	\$250
Motherboard repair (Power port, USB port) or replacement	\$100
Keyboard, Screen or Housing repair	\$50
Daughterboard (Power port, USB port), Trackpad, Microphone, Camera, Plastic Bezel, or Cable repair	\$30
Replacement Charger	\$30
Replacement Protective Case	\$20

Vandalism and Theft

In cases of theft, vandalism, and other criminal acts a police report must be filed by the student or parent/guardian and presented to the building principal. The student or parent/guardian must contact the building principal as soon as possible after the Chromebook is determined to be stolen, lost or vandalized so that the technology department can assist in potential recovery. If a device is deemed lost, the student or parent/guardian will notify building officials. The full replacement cost will need to be paid in full before a new device will be issued to the student.

Disclaimer of Liability

The Willoughby-Eastlake City School District makes no guarantee that the functions or services provided by or through the computer network and internet will be error free or without defect. While we make every effort to mitigate risk, the District will not be responsible for any damage you may suffer including but not limited to loss of data, interruptions of service, or exposure to offensive material. The District will not be responsible for financial obligations arising from the unauthorized use of the system.

District Policies

7540 - TECHNOLOGY

The Board of Education is committed to the effective use of technology to both enhance the quality of student learning and the efficiency of District operations.

Students' use of District Technology Resources (see definitions in Bylaw 0100) is a privilege, not a right. Students and their parents must sign and submit a *Student Technology Acceptable Use and Safety* form. (See also, Policy 7540.03)

The Superintendent shall include technology planning as part of the strategic plan.

See Policy 7540.03 and AG 7540.03 - Student Technology Acceptable Use and Safety, and Policy 7540.04 and AG 7540.04 – Staff Technology Acceptable Use and Safety.

This policy, along with the Student and Staff Technology Acceptable Use and Safety policies, and the Student Code of Conduct, further govern students' and staff members' use of their personal communication devices (see Policy 5136 and Policy 7530.02). Users have no right or expectation of privacy when using District technology resources (including, but not limited to, privacy in the content of their personal files, e-mails and records of their online activity when using the District's computer network and/or Internet connection).

Further safeguards shall be established so that the Board's investment in both hardware and software achieves the benefits of technology and inhibits negative side effects. Accordingly, students shall be educated about appropriate online behavior including, but not limited to, using social media, which is defined in Bylaw 0100 to interact with others online; interacting with other individuals in chat rooms or on blogs; and, recognizing what constitutes cyberbullying, understanding cyberbullying is a violation of Board policy, and learning appropriate responses if they experience cyberbullying.

Staff use of District-approved social media platforms/sites shall be consistent with Policy 7544.

Students must comply with Policy 5136, Policy 5722, Policy 7540.03, and Policy 7544 when using District Technology Resources to access and/or use District-approved social media.

Revised 3/22/17 © Neola 2019

7540.03 - STUDENT TECHNOLOGY ACCEPTABLE USE AND SAFETY

Technology has fundamentally altered the ways in which information is accessed, communicated, and transferred in society. As a result, educators are continually adapting their means and methods of instruction, and the way they approach student learning, to incorporate the vast, diverse, and unique resources available through the Internet. The Board of Education provides Technology Resources (as defined in Bylaw 0100) to support the educational and professional needs of its students and staff. With respect to students, District 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 limited 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 a public forum, and the Board imposes reasonable restrictions on its use consistent with its limited educational purpose.

The Board regulates the use of District Technology Resources by principles 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 Technology Resources and students' personal communication devices when they are connected to the District computer network, Internet connection, and/or online educational services/apps, or when used while the student is on Board-owned property or at a Board-sponsored activity (see Policy 5136).

Users are required to refrain from actions that are illegal (such as libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, and the like) or unkind (such as personal attacks, invasion of privacy, injurious comment, and the like). Because its Technology Resources are not unlimited, the Board has also instituted restrictions aimed at preserving these resources, such as placing limits on use of bandwidth, storage space, and printers.

Users have no right or expectation to privacy when using District Technology Resources (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity when using the District's computer network and/or Internet connection).

First, the Board may not be able to technologically limit access, through its Technology Resources, to only those services and resources that have been authorized for the purpose of instruction, study and research related to the curriculum. Unlike in the past when educators and community members had the opportunity 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), access to the Internet, because it serves as a gateway to any publicly available file server in the world, opens classrooms and students to electronic information resources that may not have been screened by educators for use by students of various ages.

Pursuant to Federal law, the Board has implemented 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. 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 Technology Resources, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. Any student who attempts to disable the technology protection measures will be subject to discipline.

The Technology Coordinator may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material, if access to such sites has been inappropriately 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 services and/or resources on the Internet 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 information and communications 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.

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 instruction for their students regarding the appropriate use of technology and online safety and security as specified above. Furthermore, staff members will monitor the online activities of students while 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.

Building principals are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying guidelines. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of District Technology Resources. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social media, including in chat rooms, and cyberbullying awareness and response. All users of District 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.

Students will be assigned a school email account that they are required to utilize for all school-related electronic communications, including those to staff members, peers, and 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, including mobile applications/apps that will be utilized by the student for educational purposes.

Students are responsible for good behavior when using District Technology Resources – i.e., behavior comparable to that expected of students when they are in classrooms, school hallways, and other school premises and school sponsored events. 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 Technology Resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

Students may only use District 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 of District Technology Resources that are not authorized by this policy and its accompanying guidelines.

The Board designates the Technology Coordinator as the administrator responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to students' use of District Technology Resources.

Revised 12/8/14 © **Neola 2017**

7540.06 - **DISTRICT-ISSUED STUDENT E-MAIL ACCOUNT**

Students assigned a school e-mail account are required to utilize it for all school-related electronic communications, including those to staff members and 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, including mobile applications/apps that will be utilized by the student for educational purposes.

This policy and any corresponding guidelines serve to establish a framework for student's proper use of e-mail as an educational tool.

Personal email accounts on providers other than the District's e-mail system may be blocked at any time if concerns for network security, SPAM, or virus protection arise. Students are expected to exercise reasonable judgment and prudence and take appropriate precautions to prevent viruses from entering the District's network when opening or forwarding any emails or attachments to e-mails that originate from unknown sources.

Students shall not send or forward mass emails, even if educationally-related, without prior approval of their classroom teacher or the Technology Director.

Students may join list serves or other email services (e.g. RSS feeds) that pertain to academic work, provided the emails received from the list serves or other email services do not become excessive. If

a student is unsure whether s/he has adequate storage or should subscribe to a list serv or RSS feed, s/he should discuss the issue with his/her classroom teacher, the building principal or the District's Technology Director. The Technology Director is authorized to block email from list servs or e-mail services if the emails received by the student becomes excessive.

Students are encouraged to keep their inbox and folders organized by regularly reviewing e-mail messages and purging emails once they are read and no longer needed for school.

Unauthorized Email

The Board does not authorize the use of its Technology Resources, including its computer network ("network"), to accept, transmit, or distribute unsolicited bulk e-mail sent through the Internet to network email accounts. In addition, Internet e-mail sent, or caused to be sent, to or through the network that makes use of or contains invalid or forged headers, invalid or non-existent domain names, or other means of deceptive addressing will be deemed to be counterfeit. Any attempt to send or cause such counterfeit e-mail to be sent to or through the network is unauthorized. Similarly, e-mail that is relayed from any third party's email servers without the permission of that third party, or which employs similar techniques to hide or obscure the source of the e-mail, is also an unauthorized use of the network. The Board does not authorize the harvesting or collection of network e-mail addresses for the purposes of sending unsolicited e-mail. The Board reserves the right to take all legal and technical steps available to prevent unsolicited bulk e-mail or other unauthorized email from entering, utilizing, or remaining within the network. Nothing in this policy is intended to grant any right to transmit or send email to, or through, the network. The Board's failure to enforce this policy in every instance in which it might have application does not amount to a waiver of its rights.

Unauthorized use of the network in connection with the transmission of unsolicited bulk e-mail, including the transmission of counterfeit e-mail, may result in civil and criminal penalties against the sender and/or possible disciplinary action.

Authorized Use and Training

Pursuant to Policy 7540.03, students using the District's e-mail system shall acknowledge their review of, and intent to comply with, the District's policy on acceptable use and safety by signing and submitting Form 7540.03 F1.

Furthermore, students using the District's e-mail system shall satisfactorily complete training, pursuant to Policy 7540.03, regarding the proper use of e-mail.

© Neola 2017