Reavis High School
District 220
Chromebook Handbook

Procedures and Information
2016-17

Use of Technology

All students in grades 9-11 will be issued Dell 11 Chromebooks for educational use in school and at home. This document provides students and their parents/guardians with information about the general use of technology, ownership of the devices, rights and responsibilities for possession of the device, educational use, care of the Chromebook and being a good digital citizen.

Students and their parents/guardians are reminded that use of school technology is a privilege and not a right and that everything done on any school-owned computer, network, or electronic communication device may be monitored by school authorities. Inappropriate use of school technology can result in limited or banned computer use, disciplinary consequences, removal from courses, loss of credit, receiving a failing grade, and/or legal action as stated in Student Code of Conduct. To understand the technology use expectations, students and their parents/guardians are responsible for reviewing Reavis High School's Acceptable Use Policy.

Ownership of the Chromebook

All school-issued Chromebooks and accessories are the property of Reavis High School and the school lends the Chromebook to the students for educational purposes only for the academic year. Additionally, Reavis administrative staff and faculty retain the right to collect and/or
inspect Chromebooks at any time, including via electronic remote access, and to alter, add or delete installed software or hardware.

Receiving Your Chromebook

Students will receive their Chromebooks on schedule pick-up days and need to sign all required documents on schedule pick-up day before they will be issued their device. Students will view a Chromebook training video during the first week of school.
Parents are encouraged to attend a Chromebook orientation night held at the school on multiple evenings in early fall.

Returning Your Chromebook

End of Year

At the end of the school year, students will turn in their Chromebooks and all peripherals and accessories. Failure to turn in a Chromebook will result in the student being charged the full $350.00 replacement cost.

Transferring/Withdrawing Students

Students that transfer out of or withdraw from Reavis High School must turn in their Chromebook and accessories to the IT Department on their last day of attendance. Failure to turn in the Chromebook will result in the student being charged the $350.00 replacement cost. Unpaid fines and fees of students leaving Reavis High School may be turned over to a collection agency.

Rights and Responsibilities

Content Filter

The district utilizes an internet content filter that is in compliance with the federally mandated Children's Internet Protection Act (CIPA). All Chromebooks, regardless of physical location (in or out of school), will have all internet activity protected and monitored by the district. Essentially, if a website is blocked in school, then it will be blocked out of school as well. If an educationally valuable site is blocked, students should contact their teachers to request the site be unblocked. Parents/guardians are responsible for filtering and monitoring any internet connection students receive that is not provided by the school.

No Expectation of Privacy

Students should have no expectation of confidentiality or privacy with respect to any usage of a Chromebook, regardless of whether that use is for school-related or personal purposes, other than as specifically provided by law. The school may, without prior notice or consent, log, supervise, access, view, monitor, and record use of student Chromebooks at any time for any reason related to the operation of the school. By using a Chromebook, students agree to such access, monitoring, and recording of their use.

Monitoring Software

Teachers, school administrators, and the technology department staff may use monitoring software that allows them to view the screens and activity on student Chromebooks.

Operating System and Security

Students may not use or install any operating system on their Chromebook other than the current version of ChromeOS that is supported and managed by the school.

Updates

The Chromebook operating system, ChromeOS, updates itself automatically. Students do not need to manually update their Chromebooks.

Google Apps for Education

Chromebooks seamlessly integrate with the Google Apps for Education suite of productivity and collaboration tools. This suite includes Google Drive, Docs, Sheets, Slides, Drawings, and Forms. All work is stored in the cloud.

Chrome Web Apps and Extensions

Students are allowed to install appropriate Chrome web apps and extensions from the Chrome Web Store. Students are responsible for the web apps and extensions they install on their Chromebooks. Inappropriate material will result in disciplinary action. Some web apps will be available to use when the Chromebook is not connected to the internet.

Chromebook Identification

The district will maintain a log of all Chromebooks that includes the Chromebook serial number, asset tag code, and name and ID number of the student assigned to the device. The asset tag sticker is located on the bottom of the Chromebook and must remain on the Chromebook at all times. Chromebooks without an asset tag sticker will be confiscated by Reavis faculty and/or staff and returned to the IT Department and the deans will be notified of the student associated with the device.

Using Your Chromebook At School

Charging Chromebooks

- Students are expected to bring a fully charged Chromebook to school every day and bring it to all classes unless specifically advised not to do so by their teacher.
- Students should bring their Chromebook home every day and charge it every evening.
- An uncharged Chromebook is in violation of this agreement.
- The IT Department will have a limited number of loaner Chromebooks for students who either come to school with an uncharged Chromebook or forget the device at home.
- Students who repeatedly come to school without their Chromebook or with an uncharged Chromebook may face disciplinary action.

Chromebooks being repaired

- Loaner Chromebooks may be issued to students when they leave their school-issued Chromebook for repair.
- A student borrowing a Chromebook must sign a loaner agreement and will be responsible for any damage to or loss of the loaned device.
- Chromebooks on loan to students having their devices repaired may be taken home.

Backgrounds/Themes/Sound

- Inappropriate media may not be used as Chromebook backgrounds or themes. The presence of such media will result in disciplinary action.
- Sound must be muted at all times unless permission is obtained from a teacher.
- Headphones may be used at the discretion of the teacher.
- Students should have their own personal set of headphones for sanitary reasons.

Printing

- Students will be encouraged to digitally publish and share their work with their teachers and peers when appropriate.
- Because all student work should be stored in an Internet/cloud-based application (Google Drive), student printing will be limited to a few printers located throughout the school.

Logging into a Chromebook

- Only a Reavis Google Apps for Education account may be used when students sign into their Chromebooks.
- Students should never share their account passwords with others, unless requested by a teacher/administrator.

Managing and Saving Your Digital Work With a Chromebook

- The majority of student work will be stored in an Internet/cloud-based application (Google Drive) and can be accessed from any computer with an Internet connection and most mobile devices.
- Some files may be stored on the Chromebook's hard drive.

Using Your Chromebook Outside of School

Students are encouraged to use their Chromebooks at home and other locations outside of school. A WiFi Internet connection will be required for the majority of Chromebook use. However, some applications can be used while not connected to the Internet. Students are bound by the Reavis High School Acceptable Use Policy, Administrative Procedures, and all other guidelines in this document wherever they use their Chromebooks.

Chromebook Care

Taking Care of Your Chromebook

Students are responsible for the general care of the Chromebook they have been issued by the school. A Chromebook that breaks must be reported to a teacher or administrator as soon as possible so that it can be taken care of properly. A school-owned Chromebook should NEVER be taken to an outside computer service for any type of repairs or maintenance. Students should never leave their Chromebook unattended except locked in their hallway locker.

General Precautions

- Cords, cables, and removable storage devices must be inserted carefully into the Chromebook.
- The Chromebook should not be used or stored near pets.
- No food or drink should be next to the Chromebook.
- The Chromebook should not be used with the power cord plugged in when the cord may be a tripping hazard.
- The Chromebook must remain free of any writing, drawing, stickers, and labels.
- Heavy objects should not be placed on top of the Chromebook.

Carrying Chromebooks

- Never lift the Chromebook by the screen.
- Always transport the Chromebook with care and with the screen closed.

Screen Care

The Chromebook screen can be damaged if subjected to heavy objects, rough treatment, some cleaning solvents, and other liquids. The screens are particularly sensitive to damage from excessive pressure, heat, and light.

- Do not put pressure on the top of a Chromebook when it it closed.
- Do not store a Chromebook with the screen open.
- Make sure there is nothing on the keyboard before closing the lid (ie: pens, pencils, head phones).
- Only clean the screen with a soft, dry microfiber cloth or anti-static cloth.

Chromebooks left unattended

Under no circumstances should Chromebooks be left in unsupervised areas. These areas include, but are not limited to, the school grounds, the lunchroom, vehicles, bathrooms, computer labs, library, unlocked classrooms, and hallways. Any Chromebook left in these areas is in danger of being stolen. If a Chromebook is found in an unsupervised area, it should be taken immediately to the dean’s office or Chromebook Depot. Multiple offenses of leaving one’s Chromebook unattended could result in disciplinary action.

Warranty and Insurance

The annual $50 device fee will cover the warranty and insurance for the Chromebook. This will include repairing or replacing damaged equipment resulting from accidents and normal use. Abuse or neglect of the device that results in damages may be the financial responsibility of the student to repair. In case of theft, vandalism, or other criminal acts, a police report MUST be filed with the local police department and a copy submitted to the IT Department before the student will be issued a replacement Chromebook.

Reavis Technology Acceptable Use Policy

Introduction

Reavis High School recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st century technology and communication skills.

To that end, we provide access to various technologies, network systems, and internet access for student and staff use. This Acceptable Use Policy outlines the guidelines and behaviors that users are expected to follow when using school technologies or when using personally owned devices on the school campus.

- Reavis High School's network is intended for educational purposes. It is not a public access service or a public forum.
- All activity over the network or when using district technologies may be monitored and retained. Access is a privilege, not a right.
- Access to online content and posting of content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Students and staff are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of school resources can result in disciplinary action.
- Reavis High School makes a reasonable effort to ensure users' safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.
- Users of the district network or other technologies are expected to alert IT staff immediately of any concerns for safety or security.

Technologies Covered

Reavis High School may provide Internet access, desktop computers, mobile computers or devices, video conferencing capabilities, online collaboration capabilities, message boards, email, network systems and internet access. The district will attempt to provide access to new technologies as they emerge. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

Electronic Resources

The district views the use of electronic resources as central to the delivery of its educational program, and as such maintains the expectation that all students will use electronic resources as an essential part of their learning experiences. It is the policy of Reavis High School to maintain an environment that promotes ethical and responsible conduct in all electronic resource activities by staff and students. The amount of time and type of access available for each student and

staff member may be limited by the district's technology and the demands for the use of

the district's technology. These procedures are written to promote appropriate and responsible technology use in support of the mission and goals of Reavis High School. Although reasonable efforts will be made to make sure students will be under supervision while on the network, it is not possible to constantly monitor individual students and what they are accessing on the network. Some students may encounter information that may not be of educational value and/or may be inappropriate. It shall be a violation of this policy for any employee, student, or other individual to engage in any activity that does not conform to the established purposes and general rules for the use of electronic resources.

Web Access

Reavis High School provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow district protocol to alert an IT staff member or submit the site for review.

Email

Reavis High School may provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies. Email accounts should be used responsibly. Users should not attempt to open files or follow links from unknown or untrusted origin. Users are expected to communicate with the same appropriate and courteous conduct online as offline. Email usage may be monitored and archived. All communications and information accessible via electronic resources should be assumed to be public records and,

barring a privilege, they will be disclosed.

Social Networking and Collaborative Content

Recognizing the benefits collaboration brings to education, the district may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. Users are expected to communicate with the same appropriate and courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally identifying information online.

The district recognizes the importance of social media for its employees, and acknowledges that its employees have the right under the First Amendment, in certain circumstances, to speak out on matters of public concern. However, the Board will regulate the use of social media by employees, including employees' personal use of social media, when such use:

1. Interferes with the work of the school district;
2. Is used to harass coworkers or other members of the school;
3. Breaches confidentiality obligations of school district employees;
4. Disrupts the work of the school district;
5. Harms the good-will and reputation of the school district in the community; or

6. Violates the law, board policies and/or other school rules and regulations.

Mobile Devices Policy
Reavis High School may provide users with mobile computers such as a laptop or Chromebook to promote learning outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network and are expected to treat these devices with care and caution. Users should report any loss, damage, or malfunction to IT staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse. Use of school-issued mobile devices off the school network may be monitored.

Personally Owned Devices
Students should keep personally owned devices (including laptops, tablets, smartphones, and cell phones) put away during class time unless the teacher allows their use for educational purposes.

Security
Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If you believe a computer or mobile device you are using might be infected with a virus, alert IT. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Downloads
Users should not download or attempt to download or run an executable program (.exe) over the school network or onto school resources without express permission from IT staff. You may be able to download other file types, such as images or videos. For the security of our network, download such files only from reputable sites, and only for education purposes.

Netiquette
Users should always use the Internet, network resources, and online sites in a respectful manner and realize that among the valuable content online is unverified, incorrect, or inappropriate content. Reavis High School is not responsible for the accuracy of information users access on the Internet. Users should use trusted sources when conducting research via the Internet. Users should not post anything online that they would not want parents, teachers, future colleges or employers to see. Once something is posted online, it can be shared in ways not intended and access can become impossible to control.

Plagiarism
Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they did not create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the

original author.

Personal Safety
Users should be cautious and responsible when providing personal information, including phone number, address, social security number, birthday, or financial information, over the Internet. Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. All messages, comments, images, or any online content that threatens personal safety should be brought to the attention of a responsible individual immediately.

Harassment
Harassment will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of harassment. Do not send emails or post comments with the intent of scaring, hurting, or intimidating someone else. Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, harassment can be a crime. Network activity can be monitored and retained indefinitely.

Examples of Acceptable Use
- Creation of files, projects, videos, web pages, podcasts, and other activities using electronic resources, in support of education and research and consistent with the mission of the district.
- Participation in electronic communication and collaboration activities such as blogs, wikis, podcasts, email, and other activities using electronic resources, in support of education and research and consistent with the mission of the district.
- Posting of student-created original educational material, curriculum related materials, and student work. Sources outside the classroom or school must be appropriately cited and all copyright laws must be followed.
- Staff use of electronic resources for incidental personal use in accordance with all district policies and guidelines.
- Connection of any personal electronic device is subject to all guidelines in this document.
- Proper codes of conduct in electronic communication must be used. Providing personal information is inappropriate; when using electronic communications, extreme caution must always be taken in revealing any information of a personal nature.
- All electronic resource accounts are to be used only by the authorized owner of the account for the authorized purpose.
- All communications and information accessible via electronic resources should be assumed to be public records and, barring a privilege, they will be disclosed.
- As a representative of your school and community, exemplary behavior while using electronic resources should be practiced.

Examples of Unacceptable Use

- Providing unauthorized personal information such as an address or phone number.
- Contributing to cyberbullying, hate mail, chain letters, harassment, discriminatory remarks, and other antisocial behaviors.
- Using profanity, obscenity, racist terms, or other language that may be offensive to another user.
- Any use of the electronic resources for individual profit or gain; for product advertisement; for political action or political activities; or for excessive personal use.
- Playing games, accessing social networking sites, and streaming or downloading audio and video files unless specifically authorized by a teacher for instructional purposes.
- Intentionally seeking information on, obtaining copies of, or modifying files, other data, or passwords belonging to other users, or misrepresenting other users on the electronic resources.
- Using an electronic resources account authorized for another person.
- Making use of the electronic resources in a manner that serves to disrupt the use of the network by others.
- Destroying, modifying, or abusing hardware and/or software.
- Unauthorized downloading or installation of any software for use on Reavis High School electronic resources.
- Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner. Exceptions are made when duplication and/or distribution of materials for educational purposes is permitted when such duplication and/or distribution would fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC).
- Using electronic resources to access or process pornographic material, inappropriate files, or files dangerous to the integrity of the network. Accessing any material that is inappropriate for minors including products or services that the possession and/or use of by minors is prohibited by law.
- Malicious use of the electronic resources to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system.
- Any attempts to defeat or bypass the district's Internet filter by using or trying to use proxies, https, special ports, modification to district browser settings or any other techniques, designed to avoid being blocked from inappropriate content or to conceal Internet activity.
- Using any electronic resources for unlawful purposes.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technology.

Student Responsibilities

- Students should use emerging communications and collaboration tools to create and personalize networks of experts to inform their education process.

- Students should engage in technology-enabled learning experiences that transcend the classroom walls and are not limited by resource constraints, traditional funding streams, geography, community assets or even teacher knowledge or skills.
- Students see the use of relevancy-based digital tools, content and resources as a key to driving learning productivity, not just about engaging students in learning.

Staff Responsibilities

- Staff members who supervise students, control electronic equipment, or otherwise have occasion to observe student use of said equipment shall make reasonable efforts to monitor the use of this equipment to assure that it conforms to electronic resources procedures as well as with the mission and goals of Reavis High School.
- Staff should make reasonable efforts to become familiar with the electronic resources and their use so that effective monitoring, instruction, and assistance may be provided.

Rights and Responsibilities

Reavis High School recognizes its obligation to protect the well-being of students in its charge. To this end, the district retains the following rights:

- To log electronic resource use and to monitor fileserver space utilization by users, and assume no responsibility or liability for files deleted due to violation of fileserver space allotments.
- To monitor the use of electronic resource activities. This may include real time monitoring of network activity and/or maintaining a log of Internet activity for later review. The district has the right, but not the duty, to monitor any and all aspects of its technology, network systems, and internet access, including, but not limited to sites students and staff visit on the internet and reviewing email.
- To provide internal and external controls as appropriate including the right to determine who will have access to district owned equipment.
- To exclude those who do not abide by the district's electronic resources policy or other policies governing the use of school facilities, equipment, and materials. A user account may be closed at any time based upon the district's determination that a user has violated this policy.
- To provide guidelines and make reasonable efforts to train staff and students in acceptable use and policies governing electronic resource communications.
- To monitor and maintain mailing list subscriptions and to delete files from the personal mail directories to avoid excessive use of file server hard disk space. To use filtering software to block or filter access to visual depictions that are obscene and all child pornography in accordance with CIPA. Other objectionable material may be filtered. The determination of what constitutes "objectionable" material is a local decision determined by the district's educational goals.
- Reavis High School cannot be held accountable for the information that is retrieved via electronic resources.

- Even if students have NOT been given access, they may still be exposed to information from the district's computers, network systems, and/or the internet in the guided curricular activities at the discretion of their teachers.
- Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq.), notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications. Network administrators have access to all email and will monitor messages. Messages relating to or in support of illegal activities will be reported to the appropriate authorities. Students and staff waive any right to privacy in anything they create, store, send, disseminate or receive on the district's technology and network systems, including the Internet.
- The district reserves the right to monitor, inspect, copy, review, and store without prior notice any and all usage of: the network; user files and disk space utilization; user applications and bandwidth utilization; user document files, folders, and electronic communications; email; Internet access; and any and all information transmitted or received in connection with network and/or email use.
- All such information files shall be and remain the property of the district, and no student or staff user shall have any expectation of privacy regarding such materials. The district reserves the right to disclose any electronic message to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Illinois.
- Electronic backup is made of email for the purpose of public disclosure requests and disaster recovery. Barring power outage or intermittent technical issues, backups are made of staff and student files on district servers for recovery of accidental loss of deleted files. Recovery is not guaranteed.
- Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites. While Reavis High School employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.
- The district will not be responsible for any damages users may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by our own negligence or user errors or omissions. Use of any information obtained is at the user's own risk.
- The district will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.
- The district does not warranty that its technology, network systems or internet access will be secure and free of viruses, spyware and/or malware at all times.
- The district is not responsible for the content of any advice or information received by a user or any costs or charges incurred as a result of seeking or accepting any information;
  any costs, liability, or damages caused by the way the user chooses to use his or her access to the electronic resources are the responsibility of the user.

- The district will not be responsible for any damages relating to the loss of data, delays, non-deliveries, misdeliveries or service interruptions caused by negligence or omission.
- The district is not responsible for the accuracy of information users access on the Internet and is not responsible for any unauthorized charges students or staff members may incur as a result of their use of the district's technologies. Any risk and/or damages resulting are assumed by and is the responsibility of the user.
- The district reserves the right to change its policies and rules at any time without notification. The interpretation, application, and modification of this policy is within the sole discretion of the district. Any questions or issues regarding this policy should be directed to the Superintendent.

Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including, but not limited to:

- Suspension of network, technology, or computer privileges
- Notification to parents/supervisors
- Detention or suspension from school and school-related activities
- Legal action and/or prosecution

Appropriate disciplinary repercussions will be determined on a case-by-case basis and will be based upon the nature and seriousness of the individual incident.

Digital Citizenship

While working in a digital and collaborative environment, students should always conduct themselves as good digital citizens by adhering to the following:

1. **Respect Yourself:** I will show respect for myself through my actions. I will select online names that are appropriate. I will use caution with the information, images, and other media that I post online. I will carefully consider what personal information about my life, experiences, or relationships I post. I will not be obscene. I will act with integrity.
2. **Protect Yourself:** I will ensure that the information, images, and materials I post online will not put me at risk. I will not publish my personal details, contact details, or a schedule of my activities. I will report any attacks or inappropriate behavior directed at me while online. I will protect passwords, accounts, and resources.
3. **Respect Others:** I will show respect to others. I will not use electronic mediums to antagonize, bully, harass, or stalk people. I will show respect for other people in my choice of websites: I will not visit sites that are degrading to others, pornographic, racist, or inappropriate. I will not enter other people's private spaces or areas.
4. **Protect Others:** I will protect others by reporting abuse and not forwarding inappropriate materials or communications. I will avoid unacceptable materials and conversations.
5. **Respect Intellectual Property:** I will request permission to use copyrighted or otherwise protected materials. I will suitably cite all use of websites, books, media, etc. I will acknowledge all primary sources. I will validate information. I will use and abide by the fair use rules.

6. **Protect Intellectual Property:** I will request to use the software and media others produce. I will purchase, license, and register all software or use available free and open source alternatives rather than pirating software. I will purchase my music and media and refrain from distributing these in a manner that violates their licenses.