



**RIVERVIEW SCHOOL DISTRICT
STUDENT TECHNOLOGY
HANDBOOK**

2022-2023

Introduction

The goal of the Riverview School District is to provide the best education possible by providing all students with the technology tools and preparation to be both college and/or career ready. The Riverview School District 1:1 Technology Initiative has the opportunity to provide its students with a tool to help actively engage all students in their learning.

Issuing Computers to High School Students

~~After attending the Parent/Student Orientation,~~ Students in grades 9-12 will be issued a MacBook Air, charging cables, and a carrying case. The laptop will be assigned to individual students and serial numbers recorded and this will stay with the student for the remainder of the school year in which it was issued, or until the student withdraws from school. Students will be issued the same laptop from year to year. Students are responsible for bringing the laptops to school, taking them home each day, and charging them for use the next day. The laptops are not to be left unsupervised at school or at home in unsecured locations.

Terms of MacBook Loan

~~Parent/guardian(s) will be informed of the date and time of a mandatory orientation meeting. The program and Student/Parent Laptop agreement will be explained at the mandatory orientation meeting. The parent/guardian(s) and student must sign the agreement in order for the student to be issued a MacBook.~~

A. Terms of Loan (High School)

1. Riverview School District will issue a MacBook to students in grades 9-12 upon compliance with the following:
 - ~~Completion of Parent/Guardian Orientation Meeting session~~
 - ~~Completion of Student Orientation Training Session~~
 - Submission of signed Student Acceptable Use of Technology Agreement
 - Submission of signed Student/Parent Laptop Agreement
2. Students may be subject to loss of privilege, disciplinary action and/or legal action in the event of intentional damage and/or violation of policies and guidelines as outlined in the Student/Parent ~~Netbook~~ Handbook as well as the Riverview School District Acceptable Use Policy.
3. A student's possession of the MacBook terminates no later than the ~~first~~ last day of final exams, unless there is a reason for earlier termination determined by the principal.

Transporting Computers

The Riverview School District will supply each student with a carrying case for his or her assigned computer. This case is designed to protect the computer and accessories assigned to the student.

- Anytime a computer is transported, even between classes, the computer must be in the case provided to the student.
- Computers must remain in their cases when students are being transported on a bus.
- All laptop and components are to be carried in the school-provided laptop carrying cases at all times. Do not put laptops, without the school provided carrying case, in another bag.
- If the computer remains in the provided case, the case with the computer in it can be carried in a larger backpack or messenger bag.
- Laptops should always be shut down or placed in standby mode/hibernate mode before being placed in the carrying case in order to prevent hard drive damage.
- Always close the lid before moving or carrying the laptop.
- Do not leave the laptop in visible sight in a vehicle.
- Carefully unplug all cords, accessories, and peripherals before moving the laptop or placing it into the case.
- Do not overload the laptop carrying case since this is likely to cause damage to the laptop. Textbooks, notebooks, binders, pens, pencils, etc. are not to be placed in the laptop carrying case.

Skins

Students are not only allowed to put a skin on their MacBook, they are encouraged to use a skin for additional protection. Skins for the 11" or 13" MacBook Air can be purchased through many online retailers and can be plain or customized for your student's preference. The skin is a **plastic shell** which encases the entire MacBook and adds an additional layer of protection. **No stickers will be allowed on MacBooks.** Please see your campus administrator or tech department for questions.

Loaning Equipment to Others

Students may not lend laptops or laptop components to others for any reason. This includes other family members. Parents/legal guardians may use the laptops to

assist their child who is assigned the laptop with homework and school assignments, to check students grades, and/or to communicate with teachers regarding their child.

Power Management

It is the student's responsibility to recharge the laptop battery so it is fully charged at the beginning of each school day. Power outlets may not be accessible in classrooms for recharging.

Uncharged batteries or failure to bring the laptop to class will not be an acceptable excuse for late or incomplete work or inability to participate in class activities.

When charging the laptop, make sure cords are out of the way to avoid anyone tripping over them.

All students are required to carry their chargers (AC adapters) to school to recharge the battery if necessary.

Protect the laptop by using a surge protector whenever possible.

Conserving Battery Power

- 1) Use standby mode or hibernate mode throughout the day.
- 2) Dimming the brightness of the screen will extend battery run time.
- 3) For prolonged periods of inactivity, shutdown the laptop.
- 4) Do not drain the battery down to 0%. Keep a well-charged battery at all times and plug in when needed.

Student Storage/Saving Files

Students are responsible for maintaining and backing up their files and documents. Any files saved to the laptop hard drive may be lost in the event of a hardware failure or may be removed during maintenance. At the end of the school year, all student files on the laptop hard drive will be deleted.

Students may backup to external devices, such as a thumb drive, or students may backup to "cloud" storage on the web, such as Google Drive. If the student laptop crashes and files are lost, it is the student's responsibility to have the files saved elsewhere.

Please note: "The computer crashed." is not an acceptable excuse for late assignments.

Access/Media Center/Library

Students will be allowed access to the Internet at school through the school's network and every attempt will be made to supervise and filter content students may access.

If available, students may also access the Internet outside school by connecting to a wireless network. A student's access to content outside the school network will not be filtered. Parents are encouraged to supervise their child's use of the laptop. If a parent suspects any inappropriate activity, they may contact the principal's office and have our technical staff examine the content on the laptop to determine if students are accessing inappropriate content.

~~Riverview School District recognizes that all students may not have access to a wireless Internet connection outside school, so the library hours at Riverview High School will be extended at least two days per week to allow students access to the Internet. This will be accomplished through the 21st Century Afterschool Program and Credit Recovery Program. A schedule of extended library hours will be sent home with students and posted on the school website at www.riverviewsd.org.~~

Day Users

The Riverview School District created our 1:1 Laptop Initiative to allow all students access throughout the school day and beyond to the latest technology that will help prepare them for a technology driven world. To have the greatest influence on our student's education, the Riverview School District recommends that parents allow students to take their assigned laptop home.

The district also understands that some parents may not want their student to bring their assigned laptop home for various reasons. In this event, the student can be designated as a "Day User" and students will check-out their laptop at the beginning of the day and check it back in at the end of the day.

Students may also be assigned a "Day User" status if they demonstrate that they are not responsible with their laptop. The determination to change a student's status to a "Day User" status will be at the discretion of the school administration.

Email and Internet Use

Email and other Digital Communications Accounts

Students are provided an email account by the school. Email correspondence will be used for educational purposes only. Electronic communication coming from or going to the school-issued email account can and will be monitored to make sure the terms of the acceptable use policy (AUP) are being followed.

Digital communications etiquette is expected by all students using all

school-provided communications accounts, sites, or applications including but not limited to wikis, blogs, forums, interactive video conferencing, podcasts, vodcasts, online training, online courses, and online collaboration sites.

Internet Use

As required by the **Children's Internet Protection Act (CIPA)**, an internet filter is maintained by the district for school use on the laptop. Filtering not only restricts access to unacceptable sites, but also restricts access to inappropriate materials of all kinds. Riverview School District cannot guarantee that access to all inappropriate sites will be blocked. No filter is as reliable as adult supervision!

Log files are maintained on each laptop with a detailed history of all sites accessed. It is the responsibility of the user to appropriately use the laptop, network, and the Internet. Riverview School District will not be responsible for any harm suffered while on the network or the Internet.

There is no way for the Riverview School District to effectively filter content while students are using their device at home; therefore, parents must be aware of their student's computer activity. Adult supervision is the most effective means of filtering content from the Internet.

Students are required to notify a teacher or administrator if they access information or messages that are inappropriate, dangerous, threatening, or make them feel uncomfortable.

Internet Safety

As a part of the Riverview School District curriculum, students will be instructed about appropriate online behavior, including interacting with other individuals on social networking web sites and in chat rooms. Lessons will also be provided to create an environment free of cyberbullying in compliance with Arkansas State Law.

Students Must:

- 1) Immediately report any unauthorized activity on the network or Internet.
- 2) Notify a teacher immediately if you accidentally access an inappropriate site.
- 3) Never read someone else's email or open their files or folders without permission
- 4) Never use or transmit anything with racist, abusive, threatening, demeaning, slanderous, objectionable, sexually explicit, or inflammatory content.
- 5) Never arrange to meet an Internet contact in person.

6) Observe all copyright laws; do not claim authorship of work copied from a web site or from any other source; accurately cite sources of information.

7) Protect your user account by keeping your password secure and logging off or locking when not at the computer. All email, network, and Internet activity is the responsibility of the individual whose account is logged in to the computer at the time of the activity. If your account is logged in, you are responsible. Keep any passwords a secret.

8) Protect personal information. Never give full name, addresses, phone numbers, passwords, and social security numbers for yourself and/or others. Use a “code name” that does not identify you personally to online viewers/organizations you do not know.

9) Avoid online sites and materials that do not support the curriculum or are otherwise inappropriate for educational use.

Monitoring and Supervision

Riverview School District engages students in an Internet Safety program and instructs students in making appropriate choices regarding Internet use, content evaluation and web site selection. The Riverview School District also takes technical measures to filter Internet access to protect students from inappropriate content. School-district personnel supervise student use of technical resources, including Internet browsing. These measures are in place to protect students and help them become informed consumers of Internet content. However, no technical measure or human supervision is failsafe. While we are committed to protecting our students, we acknowledge students may access inappropriate content, intentionally or accidentally. Ultimately it is the responsibility of the student to practice internet safety measures and use the resources to access appropriate educational resources.

Riverview School District does not recommend that students use laptops in an unsupervised or isolated setting while off campus. Riverview School District recommends students use laptops in plain view of parents, guardians, or other family members.

Students will provide access to the laptop and any accessories assigned to them upon request by the school or district. A search of the laptop and student files may be conducted at any time if there is suspicion that any policies, procedures, or guidelines have been violated.

While at school, the Riverview School District Technology Coordinators have the ability to remotely monitor student computer use.

Privacy

There is no expectation of privacy regarding the contents of computer files or communication using any school-owned computer or network. Riverview School District reserves the right to investigate, review, monitor, and restrict information stored on or transmitted via Riverview School District's equipment. Parents, guardians, and students do not have the right or expectation of privacy for any use of school-owned laptops, computers, or other equipment.

School-system personnel may conduct an individual search of the laptop, files, music, videos, emails or other related items. The district will cooperate fully with local, state, or federal officials in investigations of suspected illegal activities conducted through district-owned computer systems.

Passwords

Students should log in only under their assigned username and password. Students should not share their passwords with other students.

Laptop Inspections

Students may be randomly selected to provide the laptop for inspection. Students with damaged laptops who fail to report the damage will be subject to additional fines and disciplinary action.

Student Responsibilities

Students are responsible at all times for the laptops, whether at school or off campus. The student assigned the laptop is responsible for all use of the laptop. Unsupervised laptops will be confiscated by staff and taken to a designated office. Students must see an administrator in order to retrieve the unsupervised laptop. Disciplinary action may be taken for repeat offenders.

Students are required to bring the laptop to school each day with a fully charged battery. Students must bring the laptop to all classes, unless specifically instructed not to do so by their teacher. A laptop left at home is not an acceptable excuse for not submitting work; a reduction in a grade may be given. A lost document is not an excuse for late or missing work. Students leaving laptops at home will be required to complete assignments using alternate means determined by the teacher. Students will not be given the use of a loaner laptop if he or she leaves the laptop at home; ~~however, the student will have access to desktop computers in the classroom.~~ Disciplinary action may be taken for students who repeatedly leave a laptop at home.

Users are responsible for their actions and activities involving school-owned computers, networks and Internet services, and for their files, passwords, and accounts on school-owned equipment. Students must ask for assistance if they do

not know how to operate technology that is required in a class. Students are responsible for their ethical and educational use of all computer hardware and software. Students should monitor all activity on their account(s) and report anything suspicious to a teacher. Students who identify or know about a security problem are required to communicate the security problem to their teacher without discussing it with other students.

The right to use a laptop at home is a privilege. If students do not adhere to Riverview School District's Responsible Use of Technology and Internet Safety Agreement, all Board policies, and the guidelines in this Student Laptop Handbook, the privilege to use the laptop at home may be restricted or eliminated. The same rules and expectations for student conduct also apply to student use of computers. Intentional misuse or neglect can result in loss of laptop use, disciplinary action, and/or fines for any needed repairs or maintenance. The school principal will have final authority to decide appropriate disciplinary action if students are found to be responsible for any unacceptable activity.

Unacceptable Behavior

Unacceptable conduct includes, but is not limited to the following:

- 1) Using the network for illegal activities, including copyright violations;
- 2) Accessing online sites or materials that do not support the curriculum or are inappropriate for school purposes while on campus;
- 3) Downloading inappropriate materials, viruses, or software;
- 4) Using or possessing hacking or file-sharing software, including keystroke loggers, batch files, or applications used to bypass laptop or network security;
- 5) Gaining unauthorized access anywhere on the network including attempting to log onto the Internet, network, servers, routers, switches, printers, or firewall as a system administrator;
- 6) Using the laptop or network for financial gain, advertising, or political influence;
- 7) Vandalizing or tampering with equipment, files, software, system performance, or other network equipment;
- 8) Attempting to repair, remove or install computer hardware or software;
- 9) Opening the computer to access internal parts;
- 10) Causing network congestion or interfering with the work of others, including sending chain emails or broadcast messages;

- 11) Subscribing to mailing lists, mass emails, games, or other services that cause network congestion;
- 12) Intentionally wasting finite Internet or network resources, including downloading files, streaming music, videos, or games or installing, activating, or creating programs that interfere with the performance of the network, Internet, or computer hardware;
- 13) Revealing, sharing, or posting personal information including full names, addresses, phone numbers, social security numbers, driver's license numbers, or passwords for yourself or others;
- 14) Invading the privacy of others;
- 15) Using another person's username or password, or allowing another to access your account using your username or password;
- 16) Pretending to be someone else when sending or receiving messages;
- 17) Using email other than the school-issued email account, on school-owned equipment;
- 18) Forwarding or distributing inappropriate email messages;
- 19) Engaging in harassment or transmitting obscene messages, pictures, websites, or other files including racist, terroristic, abusive, sexually explicit, vulgar, threatening, stalking, demeaning, slanderous, or any other inflammatory content;
- 20) Utilizing sites to sell or purchase written papers, book reports, and other student work, or to commit any act of plagiarism;
- 21) Using unauthorized technology to gain advantage on assessments by providing or receiving information not allowed by the instructor or that is unavailable to other students;
- 22) Assisting, observing, or joining any unauthorized activity using the laptop, network, or Internet;
- 23) Accessing or attempting to access Internet sites not approved by district/teacher which may include non-educational chat rooms, instant messaging, or social networking sites and may include MySpace, Facebook, YouTube and other sites that could distract from engagement in academic and school-related pursuits;
- 24) Attempting to disable or circumvent Riverview School District's Internet content filter and firewall, or attempting to use proxies to access sites that would otherwise be restricted.

- 25) Falsifying permission or identification information;
- 26) Copying or modifying files, data, or passwords belonging to others, or using technology to circumvent doing your own work for your courses;
- 27) Knowingly placing a computer virus on a computer or network (additionally, legal charges may be filed);
- 28) Writing, drawing, painting, defacing, or placing stickers or labels on school-owned laptops or laptop accessories, or causing other intentional damage;
- 29) Attempting to alter data or the configuration of a computer or the files of another user is considered an act of vandalism and subject to disciplinary action;
- 30) Presence of images of guns, weapons, pornographic materials, inappropriate language, alcohol, drugs, or gang-related symbols are subject to disciplinary action;
- 31) Cyberbullying in any form is unacceptable. Students will not engage in any cyberbullying activity, which may include efforts to harass, threaten, torment, embarrass or intimidate students or school staff through the use of a computer. In situations in which cyberbullying originates from off-campus conduct, but is brought to the attention of school officials, any disciplinary action will be based upon whether the conduct is determined to be materially and substantially disruptive of the school environment or have a direct and immediate effect on school safety or on maintaining order and discipline in the schools. Discipline for cyberbullying will be handled on a case-by-case basis as deemed appropriate by the school principal. In addition, if a criminal act has been committed, it will be reported to local law enforcement.
- 33) Students will comply at all times with Board policies, the Responsible Use of Technology and Internet Safety Agreement, and this Laptop Handbook.

Consequences

Consequences for non-compliance with the policies and procedures in these documents include disciplinary actions and financial responsibilities. Any failure to comply may immediately end the student's right to access the laptop, or other devices or services. The student will also be subject to disciplinary action as set out in the Riverview School District Student Code of Conduct. The school principal will have authority to decide appropriate consequences regarding non-compliance.

Technical Support and Repairs

Technical support/Help Desk is only available during school hours from 8am-3pm. If a student has a technical problem at home, he or she should document the problem as completely as possible recording any error messages, exactly what the student was doing at the time, and the software being used when the problem

occurred. With teacher permission, the student should report the problem to the help desk during operating hours. All repairs will be performed or managed by school district personnel. Parents, guardians, students, or teachers are not allowed to attempt repairs themselves or contract with any other individual or business to repair any school-owned computer equipment. Every effort will be made to repair or replace the laptop in a timely fashion.

Services provided include the following:

- Hardware or software maintenance and repairs
- User account support
- Operating system and software support
- Hardware support
- Updates and software installations
- Warranty repairs
- Managing laptop tracking service
- Basic troubleshooting

Help Desk Procedures:

1. Student identifies a problem.
2. Student request a teacher or staff member to submit a Tech Request. With teacher permission and a pass, the student MUST bring the laptop, bag, and charger to the designated room when authorized to do so.
3. A Help Desk Assistant will greet students with laptop problems. The problem may be fixed while the student waits.
4. If the problem requires time at the Help desk, then the teacher or paraprofessional will fill out a "Help Desk Note" with as much diagnostic info as necessary.
5. The student will take his/her laptop to the front desk and staff there will check it in, including bag and charger. The Technology staff will check out a loaner laptop to the student.
6. When the laptop is fixed, the Help Desk will notify the student that their laptop has been fixed. It is the student's responsibility to return the loaner, bag, and charger to the Media staff prior to receiving their original assigned laptop.

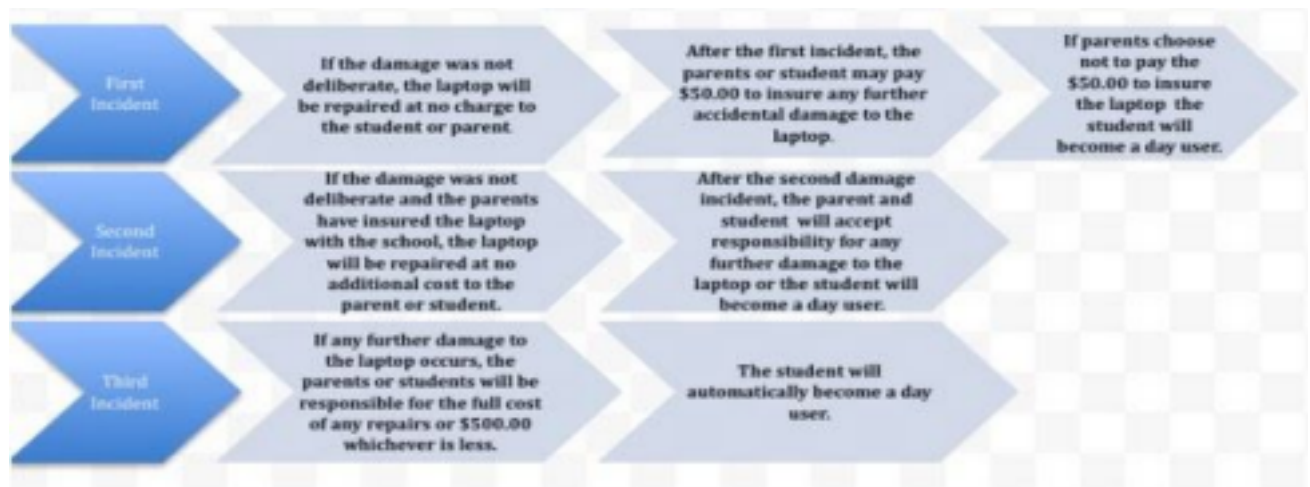
Damage, Loss or Theft

In case of theft, vandalism, and other criminal acts, the student or parent MUST file a police report within 48 hours of the occurrence.

Incidents happening off campus must be reported to the police by the parent and a copy of the report be brought to the school by the next business and/or school day.

- Students will be charged the full price of the computer or repairs if deliberately damaged or vandalized.
- If damage is negligent, student may be responsible for the reasonable cost of repair or replacement costs.
- If a transfer to another school takes place, students will have 48 hours to return the computer to its home school.
- Seniors must clear all records and pay all fees before participating in the graduation ceremony.
- Parents/Students are responsible for reasonable cost of repair for deliberately damaged computers.

What happens if you damage your laptop?



Student Work for Repairs Program

If a student damages their laptop and cannot afford either the cost of the insurance, cost of repairs, or the replacement cost, the student may work with maintenance and custodial crews after school. The students will be credited the hourly minimum wage rate of \$8.50 per hour worked towards the repair of their laptop or device. Students will be allowed to work a maximum of two hours per day.

There are a limited number of slots to work with custodial and maintenance crews. Students will be allowed to work on a first come, first serve basis. Students must sign up daily to work with the custodial and maintenance crews. A sign-up sheet will be available in the school office where a record will also be kept of all damages accrued, payments, and hours worked.

Repossession:

If you do not timely and fully comply with all terms of this Agreement and the Parent/Student Technology Handbook, including the timely return of the property, the District shall be entitled to declare you in default and come to your place of residence, or other location of the property, to take possession of the property.

Parent Expectations

1. Remember that while the school system will provide Internet content filtering, there is no substitute for parental supervision when using a computer.
2. Monitor student use of the laptop and Internet at home.
3. Ensure your child understands and adheres to laptop and Internet policies and guidelines set forth in the 1:1 Laptop Handbook.
4. *Sign a copy of the 1:1 Laptop Agreement that you will find at the end of this handbook.*
5. If the device is intentionally damaged or after the second damage incident, parents will reimburse the school district per school policy for any costs incurred due to misuse, neglect, damage, or loss, including theft, if not otherwise covered by warranty or insurance, up to the full replacement cost of the laptop.
6. Review Riverview School District's Responsible Use of Technology and Internet Safety Agreement, this 1:1 Laptop Handbook with your child.
7. Assist your child who is assigned the laptop with homework and school assignments. The purpose of the 1:1 Laptop Initiative is to help students learn. Student use of the laptop for learning is the most important priority of the 1:1 Laptop Initiative.
8. Ensure return of laptop and all accessories in good working condition at the end of the current school year or before the student withdraws from school.

Student Expectations

I Promise to...

- . be responsible for my laptop at all times.
- ~~. secure my laptop in a locker when not using my laptop for class.~~
- . carry and store my laptop in the laptop case provided by the district at all times.
- . report technical problems with my laptop to the campus repair center.
- . back-up critical files regularly in the cloud with Google Drive or Dropbox and/or a portable USB drive.
- . not share my login password with anyone.
- . not loan my laptop or any laptop component to another student for any reason.
- . not change the standardized software already loaded on the laptop. . not change the screensaver or any of the settings on the computer. . not download music, videos, games or programs, other than those used during instruction.
- . not delete any files or folders that I did not create because deletion of certain files can affect the performance of the laptop and can interfere with my ability to complete class work which may affect my grade.
- . not use my laptop while riding on the bus.

Computer Tips for Parents

Computers are a resource or tool. Riverview School District strives to prepare all students for a future in the global workplace. Our children will be faced with computer and Internet distractions in everything they do in the world today and RSD is preparing them to stay focused and handle those distractions.

Parents are still in control and have the ability to:

1. Communicate with your children and set computer limits. Here are some examples:

- I will not give out personal information such as my address, telephone number, parent's work address/telephone number, or the name and location of my school without my parent's permission.
- I will tell my parents right away if I come across any information that makes me feel uncomfortable.
- I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.
- I will never send a person my picture or anything else without first checking with my parents.

- I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away so that they can contact the principal's office.
- I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online, and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.

2. Limit the hours during the day that your child is on the computer.

3. Physically monitor student activity on the computer. We encourage parents to have their student's login and password in order to monitor their child's computer profile, as well as their assignments. If students refuse to share, their password can be reset at a parent's request.

®Google/(G) Suites User Agreement

At Riverview School District, we use G Suite for Education, and we are seeking your permission to provide and manage a G Suite for Education account for your child. G Suite for Education is a set of education productivity tools from Google including Gmail, Calendar, Docs, Classroom, and more used by tens of millions of students and teachers around the world. At Riverview School District, students will use their G Suite accounts to complete assignments, communicate with their teachers, and learn 21st century digital citizenship skills.

A notice in your technology handbook provides answers to common questions about what Google can and can't do with your child's personal information, including:

What personal information does Google collect?

How does Google use this information?

Will Google disclose my child's personal information?

Does Google use student personal information for users in K-12 schools to target advertising?

Can my child share information with others using the G Suite for Education account?

Please read it carefully, and let us know of any questions. Signing this handbook will indicate that you've read the notice and give your consent. If you don't provide your consent, we cannot create a G Suite for Education account for your child. Not having access to G Suite can negatively impact the educational experience for your child. For example, students who cannot use Google services may need to use other software to complete assignments or collaborate with peers.

NOTICE

This notice describes the personal information we provide to Google for these accounts and how Google collects, uses, and discloses personal information from students in connection with these accounts.

Using their G Suite for Education accounts, students may access and use the following “Core Services” offered by Google (described at https://gsuite.google.com/terms/user_features.html)

Gmail, Google+, Calendar, Chrome Sync, Classroom, Cloud Search, Contacts
Docs, Sheets, Slides, Forms, Drive, Groups, Hangouts, Hangouts Chat, Hangouts
Meet, Google Talk, Jamboard, Keep, Sites, and Vault

In addition, we also allow students to access certain other Google services with their G Suite for Education accounts. Specifically, your child may have access to the following “Additional Services”:

YouTube, Blogger, Google Maps, App Maker, Bookmark, Google Books, Google
News, Google Finance, Google in Your Language, Google Photos, Panoramio,
Tour Creator, Google Classroom, Google Earth, Google Groups, Google Scholar,
Google Translator, Google Voice, and Google Studio.

Google provides information about the information it collects, as well as how it uses and discloses the information it collects from G Suite for Education accounts in its G Suite for Education Privacy Notice. You can read that notice online at https://gsuite.google.com/terms/education_privacy.html You should review this information in its entirety, but below are answers to some common questions:

What personal information does Google collect?

When creating a student account, [insert name of school/district] may provide Google with certain personal information about the student, including, for example, a name, email address, and password. Google may also collect personal information directly from students, such as telephone number for account recovery or a profile photo added to the G Suite for Education account.

When a student uses Google services, Google also collects information based on the use of those services. This includes:

device information, such as the hardware model, operating system version, unique device identifiers, and mobile network information including phone number; log information, including details of how a user used Google services, device event information, and the user's Internet protocol (IP) address;
location information, as determined by various technologies including IP address, GPS, and other sensors;
unique application numbers, such as application version number; and cookies or similar technologies which are used to collect and store information about a browser or device, such as preferred language and other settings.

How does Google use this information?

In G Suite for Education Core Services, Google uses student personal information to provide, maintain, and protect the services. Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes.

[Include this section if your school provides access to Additional Services] In Google Additional Services, Google uses the information collected from all Additional Services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and its users. Google may also use this information to offer tailored content, such as more relevant search results. Google may combine personal information from one service with information, including personal information, from other Google services.

Does Google use student personal information for users in K-12 schools to target advertising?

No. For G Suite for Education users in primary and secondary (K-12) schools, Google does not use any user personal information (or any information associated with an G Suite for Education Account) to target ads, whether in Core Services or in other Additional Services accessed while using an G Suite for Education account.

Can my child share information with others using the G Suite for Education account?

At Riverview School District, we may allow students to access Google services such as Google Docs and Sites, which include features where users can share information with others or publicly. When users share information publicly, it may be indexable by search engines, including Google.

Will Google disclose my child's personal information?

Google will not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies:

With parental or guardian consent. Google will share personal information with companies, organizations or individuals outside of Google when it has parents' consent (for users below the age of consent), which may be obtained through G Suite for Education schools.

Riverview School District G Suite for Education accounts, because they are school-managed accounts, give administrators access to information stored in them.

For external processing. Google may provide personal information to affiliates or other trusted businesses or persons to process it for Google, based on Google's instructions and in compliance with the G Suite for Education privacy notice and any other appropriate confidentiality and security measures.

For legal reasons. Google will share personal information with companies, organizations or individuals outside of Google if it has a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to: meet any applicable law, regulation, legal process or enforceable governmental request; enforce applicable Terms of Service, including investigation of potential violations; detect, prevent, or otherwise address fraud, security or technical issues; protect against harm to the rights, property or safety of Google, Google users or the public as required or permitted by law. Google also shares non-personal information -- such as trends about the use of its services -- publicly and with its partners.

What choices do I have as a parent or guardian?

First, you can consent to the collection and use of your child's information by Google. If you don't provide your consent, we will not create a G Suite for Education account for your child, and Google will not collect or use your child's information as described in this notice.

If you consent to your child's use of G Suite for Education, you can access or request deletion of your child's G Suite for Education account by contacting your child's principal. If you wish to stop any further collection or use of your child's information, you can request that we use the service controls available to limit your child's access to features or services, or delete your child's account entirely. You and your child can also visit <https://myaccount.google.com> while signed in to the G Suite for Education account to view and manage the personal information and settings of the account.

What if I have more questions or would like to read further?

If you have questions about our use of Google's G Suite for Education accounts or the choices available to you, please contact [insert contact information for the school administrator]. If you want to learn more about how Google collects, uses, and discloses personal information to provide services to us, please review the [G Suite for Education Privacy Center](https://www.google.com/edu/trust/) (at <https://www.google.com/edu/trust/>), the [G Suite for Education Privacy Notice](https://gsuite.google.com/terms/education_privacy.html) (at https://gsuite.google.com/terms/education_privacy.html), and the [Google Privacy Policy](https://www.google.com/intl/en/policies/privacy/) (at <https://www.google.com/intl/en/policies/privacy/>).

The Core G Suite for Education services are provided to us under [Google's Apps for Education agreement](#).



**Riverview School District
7-12 Parent/Student Laptop Agreement**

(A signed copy of this form must be received by a school designee at the Parent/Student Orientation.)

- 1) I understand the laptop is property of Riverview School District and is assigned to me.
- 2) I will use the laptop appropriately for school purposes.
- 3) I will care for the laptop assigned to me and not leave it unsupervised or in unsecured locations.
- 4) I will not loan the laptop to another individual.
- 5) I will charge the laptop battery before each school day.
- 6) I will not use the laptop near food or drinks.
- 7) I will not disassemble any part of the laptop or attempt any repairs.
- 8) I will carry the laptop in the carrying case provided by the school.
- 9) I will not place stickers, drawings, markers, etc. on the laptop. I will not deface the serial number or inventory sticker on the laptop.
- 10) I understand that the laptop and its contents may be inspected at any time because it is school property.
- 11) I agree to return the laptop, carrying case, power cord, charger, charger cable, and any other accessories assigned to me when requested in good working condition.
- 12) I will follow the policies, procedures, and guidelines outlined in the Riverview Parent/Student Laptop Handbook and the Responsible Use of Technology and Internet Safety Agreement at all times.
- 13) I give permission for Riverview School District to create/maintain a G Suite for Education account for my child and for Google to collect, use, and disclose information about my child only for the purposes described in the notice contained in this handbook.

Student Name (Please Print): _____

Student Signature: _____ **Date:** _____

Parent Name (Please Print): _____

Parent Signature: _____ **Date:** _____

**Riverview School District
Responsible Use of Technology Policy**

Name _____ Grade _____

Riverview School District agrees to allow the student identified above ("student") to use the District's electronic media to access the Internet under the following terms and conditions:

Conditional Privilege: The student's use of the District's access to technology and the Internet is a privilege conditioned on the student's abiding by this agreement. The student agrees to follow the Acceptable Use of Technology Policy.

Acceptable Use: The student agrees that in using the District's Internet access he/she will obey all Federal and State laws and regulations. Internet access is provided as an aid to students to enable them to promote their education.

Penalties for Improper Use: If the student violates this agreement and/or the "Acceptable Use of Technology Policy" and/or misuses the Internet, the student shall be subject to disciplinary action.

Misuse includes, but is not limited to:

- a. using the Internet for any activities deemed lewd, obscene, vulgar, or pornographic as defined by prevailing community standards;
- b. using abusive or profane language in private messages on the system; or using the system to harass, insult, or verbally attack others;
- c. posting anonymous messages on the system;
- d. using encryption software;
- e. wasteful use of limited resources provided by the District, including paper;
- f. causing congestion of the network through lengthy downloads of files;
- g. vandalizing data of another user;
- h. obtaining or sending information which could be used to make ~~destruction~~ devices, guns, weapons, bombs, explosives or fireworks;
- i. gaining or attempting to gain unauthorized access to resources or files;
- j. identifying oneself with another person's name or password or using an account or password of another user without proper authorization;
- k. using the network for financial or commercial gain without District permission;
- l. theft or vandalism of data, equipment, or intellectual property;
- m. invading the privacy of individuals;
- n. using the Internet for any illegal activity, including computer hacking and copyright or intellectual property law violations;
- o. introducing a virus to, or otherwise improperly tampering with, the system;
- p. degrading or disrupting equipment or system performance;
- q. creating a web page or associating a web page with the District without proper authorization.
- r. attempting to gain access or gaining access to student records, grades, or files of students not under their jurisdiction;
- s. providing access to the District's Internet access to unauthorized individuals; t. taking part in any activity related to Internet use which creates a clear and present danger of substantial disruption of the orderly operation of the District or any of its schools; u. making unauthorized copies of computer software;
- v. improper use of computers during instructional time.

Student Signature _____ **Date** _____

Parent Signature _____ **Date** _____