CORNERSTONE STUDENTS
ACCEPTABLE USE OF TECHNOLOGY POLICY
(Updated 2024)

1.0   GENERAL POLICY:

This document formalizes the Technology Acceptable Use Policy for students and parents at Cornerstone Schools. It is the responsibility of the student and parent to read, understand and follow the policy and guidelines. Using school equipment, resources, network or devices shall constitute acceptance of the terms of the Technology Acceptable Use Policy and Guidelines.

Electronic devices deemed to be distracting to the educational environment by Cornerstone school administration are prohibited on campus. Schools will not be held responsible for the loss or theft of students' private property. Students are strongly encouraged not to bring such devices to school.

Please note: Cornerstone Schools reserve the right to amend this policy at any time.

2.0 CELL PHONES:

The use of cell phones and similar devices during instructional or class time is prohibited. All devices must be powered <u>OFF</u> during instructional and passing periods. This includes when you are outside of class with permission, on your way to the restroom or office or in the restroom. Devices that are powered off will not ring, vibrate or create any distractions to the student or their classmates.

Some Cornerstone Schools do not allow students to have cell phones on their person during the school day. Students must follow each building's specific cell phone policy.

Students must assume responsibility for their own devices. The school or District is not responsible for preventing theft, loss or damage. Devices must be kept out of site, e.g. in a purse, backpack or locker.

During class time phones should NOT be used for any purpose unless expressly directed by a staff member. This includes outgoing/incoming calls, text messaging,

calculating, picture taking, social media, Google searches, etc. Students may use their phones before school, during lunch time and after school at each school's discretion. Some schools will allow lunch time use while others will not.

Students found with their cell phone ON during class or between periods are in violation of the Cell Phone Policy. PLEASE NOTE: THIS IS A ZERO TOLERANCE POLICY. If a student is determined to be in violation of the policy, they are immediately subject to the consequences below:

CELL PHONE VIOLATION CONSEQUENCES:

- **EVERY OFFENSE:** Teacher will confiscate device and turn it into the Dean of Students. The phone will be returned only at the end of the day to a parent when they pick up their child.
- **AFTER 3rd OFFENSE:** Repeated repossessions (3 times or more) of a student's cell phone will result in additional disciplinary actions including up to three (3) days of In School Suspension (ISS).

The ONLY exceptions to the policy above are 1) during latch-key care as permitted by staff 2) during emergency circumstances expressly granted by a staff member, and 3) during teacher-led activities related directly to instruction.

Cornerstone Schools operates under a zero tolerance cell phone policy. First-time offenders are subject to immediate disciplinary action.

3.0 DESKTOPS / LAPTOPS / CHROMEBOOKS:

Cornerstone believes that all students and staff should have reasonable access to adequate technology and various information formats. It is up to the students and staff to use this educational advantage in an appropriate and responsible manner.

A. TECHNOLOGY & BULLYING

All computers and devices that connect to the internet must be used appropriately and adhere to the school's network policy. It must also be noted, by parents and students, that communications off campus can also become a problem at school. If a student inappropriately uses a device off-campus to threaten, bully, sexually harass or explicitly contact another student and it becomes a disruption on campus or in a remote classroom, the student can be disciplined. Before a student posts, texts, comments or contacts another student, they should consider the following:

- I can be suspended, expelled or arrested for my comments;
- If sexual in nature, I (and anyone else involved) can be prosecuted for child pornography, requiring registration as a "sex offender" for the rest of my life;
- Once something is on the internet there is no way to destroy it;
- Is the content I post something I want my parents or future employer to see;
- Many students that are harassed become seriously depressed and often commit suicide.

Cornerstone takes bullying and harassment seriously. Please contact Cornerstone administration if you or someone you know is being bullied or harassed by someone online or in-person.

B. PROHIBITED USES

Unacceptable uses of school computers include, but are not limited to, the following:

1. **Accessing or Communicating Inappropriate Materials** – Students may not access, submit, post, publish, forward, download, scan or display defamatory, abusive, obscene, vulgar, sexual in nature, threatening, discriminatory, harassing, bullying and/or illegal materials or messages.

2. **Illegal Activities** – Students may not use the Cornerstone computers, network and internet services for any illegal activity or in violation of any school policy, procedure or rules. Cornerstone assumes no responsibility for illegal activities of students while using school computers.

3. **Violating Copyrights or Software Licenses** – Students may not copy, download or share any type of copyrighted materials (including music, films, images or written word) without the owner's permission; or copy or download software without the express authorization of the Technology Coordinator. Unauthorized copying of software is illegal and may subject the copier to substantial civil and criminal penalties. Cornerstone assumes no responsibility for copyright or licensing violations by its students. This includes AI sources such as Open AI or Chat CPT.

4. **Plagiarism** – Students may not represent as their own work any materials obtained on the internet (such as term papers, articles, music, etc). When Internet sources are used in student work, the author, publisher and web site must be identified. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of

something found online.This includes AI sources such as Open AI or Chat CPT.

5. **Cyberbullying** – Cyberbullying will not be tolerated. Harassing, denigrating, impersonating, and cyberstalking are all examples of cyberbullying. Do not send emails or post comments with the intent of scaring, hurting, or intimidating others. 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, cyberbullying can be a crime.

6. **Misuse of Passwords/Unauthorized Access** – Students may not share passwords; use any user account/password that is not assigned to them; or attempt to circumvent network security systems.

7. **Malicious Use/Vandalism** – Students may not engage in any malicious use, disruption or harm to the school unit's computers, electronic devices, network and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses or intentional physical damage.

8. **Avoiding School Filters** – Students may not attempt to or use any software, utilities or other means to access internet sites or content blocked by the school filters.

9. **Unauthorized Access to Blogs/Social Networking Sites, Etc.** – Users may not access blogs, social networking sites, etc. prohibited by school administration or the Technology Department. Teachers and students using authorized social networking sites for educational projects or activities shall follow the age requirements and legal requirements that govern the use of social networking sites in addition to the guidelines established in this policy.

10. **Degrade System Resources** – Users shall not use the network in such a way that would degrade the performance system resources or disrupt the use of the network by others. This includes but is not limited to excessive printing, file storage, online games, and video/audio streaming not directly related to educational projects, as determined by the supervising instructor or school administrator.

11. **Unauthorized Equipment**– Users may not attach unauthorized equipment, including personal laptops, tablets, and handheld devices, to the district

network without permission from the school administration or the Technology Department.

C. PRIVACY

All computers, telephone systems, voice mail systems, email and electronic communication systems are CEG property. CEG retains the right to access, review and monitor all electronic messaging, voicemail, computer files, databases and other electronic transmissions contained in or used in conjunction with CEG's computer, telephone, email and voicemail systems.

Students should have no expectation that any information contained on such systems is confidential or private. Students must recognize that there is no assurance of confidentiality with respect to access to transmissions and files by persons outside, or from persons inside the school district.

D. CLASSROOM MANAGEMENT / ACCOUNTABILITY

Accountability is a key component to minimizing technology breakage, loss and theft. Staff and students must enforce the following classroom management practices:

1. Computers should be kept in specific rooms and charging carts and should never leave the classroom that it is assigned too, unless the student is attending a VILS school.
2. Students should be matched up to a specific computer so that breakage, loss or theft can be traced back to a specific student.
3. At the end of every class, a quick visual check should be done by the student and teacher to confirm that no obvious damage has been done to the device(s).
4. Once the visual check is complete, the device should be returned to storage, placed in the appropriate slot and plugged in for charging.

Teachers and students should work together to ensure that all devices are safe, well cared for and in good working order. If intentional or accidental breakage occurs, please notify a teacher underlined immediately. The teacher will notify the IT team. Unreported breakage will lead to a payment claim to the student's parent or guardian.

Additionally, the IT team records the room and teacher where breakage occurs. Students and teachers that fail to maintain adequate classroom management or that routinely disrespect electronic devices will receive administrative counseling and are subject to disciplinary action.

E. STUDENT SECURITY

A student is not allowed to reveal his/her full name, address, telephone number, social security number or other personal information on the Internet while using a school computer. Students should never agree to meet people they have contacted through the Internet without parental permission. Students should inform their teacher if they access information or messages that are dangerous, inappropriate or make them uncomfortable in any way.

F. SYSTEM SECURITY

Any student who identifies a security problem must notify his/her teacher immediately. The student shall not demonstrate the problem to others or access unauthorized material. Any user who attempts to breach system security, causes a breach of system security or fails to report a system security problem shall be subject to disciplinary and/or legal action in addition to having his/her computer privileges limited, suspended or revoked.

- Keep your Chromebook in the school provided secured carrying case for extra protection.
- Never carry the Chromebook while the screen is open.
- Do not transport Chromebook with the power cord inserted.
- Chromebooks should never be in vehicles or a location that is not temperature controlled.
- Chromebooks should

4.0 VERIZON INNOVATIVE LEARNING SCHOOLS (VILS)

Each of our Cornerstone middle schools (grades 6-8) have been selected to join Cohort 10 of the Verizon Innovative Learning Schools (VILS) initiative. The selection process was very rigorous and competitive and it will have a huge impact on our staff and students.

As part of the initiative, each of our MS staff and students will be equipped with an LTE-enabled Chromebook which will not only transform our resources in the classroom but will allow students to have 24/7 learning from anywhere.

Students will be responsible for bringing the Chromebooks from home to school each day and must follow a new set of procedures to ensure that each of our students can participate in the technology-driven lesson plans our staff will be developing. Students must return the device at the end of the school year or prior to leaving the network.

A. RECEIVING A VILS CHROMEBOOK

Chromebooks will be distributed during selected dates at the beginning of the school year. Each student will receive an AC charger with their Chromebook.

Cornerstone families acknowledge that all electronics are school property and must be returned by the specified date and time.

B. RETURNING A VILS CHROMEBOOK

Upon completion of the school year or prior to leaving the District, families must return any device that was assigned by the school. Families are not able to purchase the devices or keep them for any reason. Broken, lost or stolen devices must be reported immediately when the incident occurs. Students and parents should not wait until the device collection time to report any broken, lost or stolen devices. Any Chromebook, laptop or other electronic device that is issued for remote learning must be returned to the same school where it was issued.

C. TAKING CARE OF CHROMEBOOKS

Students are responsible for the general care of the Chromebook they have been issued by the school. If a Chromebook or laptop is physically damaged or experiencing a mechanical problem, the student should contact their school administration or Student Tech Team immediately.

Chromebooks that are broken, or fail to work properly, must be reported to the on-site Technology Liaison staff member or the Student Tech Team. DO NOT TAKE DISTRICT-OWNED CHROMEBOOKS TO AN OUTSIDE COMPUTER SERVICE FOR ANY TYPE OF REPAIRS.

I. **General Precautions**
- Chromebooks should never be left unattended except when locked in a secure area.
- No food or drink should be next to Chromebooks.
- Cords, cables, and removable storage devices must be inserted carefully into Chromebooks.
- Chromebooks should not be exposed to extreme temperatures, such as leaving them in a hot car or overnight during the winter.
- Heavy objects should never be placed on top of Chromebooks.

II. **Chromebook Screen Care**

The Chromebook screen is particularly sensitive and can be easily damaged if subjected to rough treatment and excessive pressure. Protect the Chromebook screen by following the rules below.

- When moving a Chromebook support it from the bottom with the lid closed.
- Clean the screen with a dry anti-static, or micro-fiber cloth. Do not use window cleaner or any type of liquid or water on the Chromebook.
- Nothing should be placed or leaned on top of a Chromebook.
- Make sure nothing is on the keyboard before closing the lid (e.g., pens, pencils, notebooks).
- Pressure should not be put on the screen either by poking it or wedging the Chromebook into a bookbag or place anything in the carrying case that will press against the cover.
- For screen adjustment do not grasp screen by wrapping hand around screen; your thumbs can shatter the screen.

III. Carrying & Storing Chromebooks

- Chromebooks must be stored safely at all times, especially during extra-curricular events.
- Chromebooks should never be shoved into a locker, placed on the boom of a pile or wedged into a book bag as this may break the screen.
- Never store your Chromebook in your carry case or backpack with the power cord inserted.

IV. Asset Tags & Logos

- All Chromebooks will be labeled with a school asset tag. Chromebook asset tags are recorded and associated with students. Chromebooks must have an asset tag on them at all times.
- Asset tags and logos may not be modified or tampered with in any way. Students may be charged or disciplined for tampering with a school asset tag logo or turning in a Chromebook without a school asset tag or logo.

D. CHROMEBOOKS LEFT AT HOME

- If students leave their Chromebook at home, they are allowed to request a loaner from their homeroom teacher. Loaners must be returned to the IT office at the end of the school day.
- Please review for more details on Loaner Chromebooks.
- If the device is forgotten at home or not charged prior to coming to school more than 3 times, the device will have to be left at school for the rest of the school year and the student will no longer have the privilege of taking home the device.

E. DIGITAL CITIZENSHIP & APPROPRIATE USE OF DEVICES

District-owned and VILS Chromebooks and devices are to only be used for educational purposes and are subject to all corresponding administrative procedures and policies as an on-site Chromebook. Students who use Chromebooks at home

are bound to the same Cornerstone Acceptable Use of Technology Policy and agree to follow all guidelines no matter where they are using the device.

F. ACCEPTABLE CHROMEBOOK USE

When Chromebooks are on-site, students must adhere to strict policies on acceptable use:

I. Photos, Screensavers, and Background Photos

- Inappropriate media may not be used as a screensaver or background.
- Images of guns, weapons, pornographic materials, inappropriate language, alcohol, drug, gang related symbols or pictures will result in disciplinary actions.
- Photos/videos require a large amount of storage space on the device. Only photos that are for an educational purpose should be saved to the device. All other photos/videos should not be taken or stored.

II. Sound, Music, Games and Programs

- Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.
- Students should have their own personal set of headphones, which may be used in the classroom at the discretion of teachers. Students should not have earbuds in their ears during class.
- Data Storage on the Chromebook is limited and should be managed by the students so that the full educational potential of the Chromebook is available. Any instance of downloading apps that have not been approved by the District is carefully monitored. Students may be directed by school personnel to remove apps, music, videos if the storage of instructional materials is compromised.

G. LOANER CHROMEBOOKS - POLICY & PROCEDURE

I. General Use & Precautions

- In the case you are unable to use your issued Chromebook for the school day, you may request from your homeroom teacher to borrow a loaner Chromebook to continue your studies.
- Loaners are to be treated as if it were your own issued Chromebook.
- Any damaged or missing loaners will be reported and followed up with disciplinary action.
- Loaners are NOT a substitute for your issued Chromebook and must be returned before you leave school. If you are having issues with your

Chromebook, please report these problems to school staff or the Student Tech Team.

II. Retrieving Your Loaner Chromebook

- All Chromebooks loaned to students will be logged to observe their frequency of request and ensure accountability for usage.
- Students must provide a detailed reasons as to why they are in need of a loaner.
- If the reason for borrowing a loaner is due to a malfunctioning/damaged Chromebook, please report this issue IMMEDIATELY to resolve the matter.
- Once complete, a loaner will be assigned for use for the rest of the day.
- Under NO circumstances should a Loaner Chromebook be taken home by the student.

III. Returning Your Loaner Chromebook

- Loaners must be returned to the IT office before the end of the day.
- Returned Chromebooks will be confirmed by the IT officer daily to ensure we have a healthy supply ready for use if need be.
- Failure to return a loaner will be met with investigation and potential disciplinary action, including removal of privileges to borrow loaners.

H. CONTENT FILTER & DEVICE MONITORING

Cornerstone Schools utilizes an Internet content filter that is in compliance with the federally mandated Children's Internet Protection Act (CIPA). https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

- All Chromebooks, regardless of physical location (in or out of school), will have all internet activity protected and monitored by the District.
- If a website is blocked at school, then it will also be blocked when a student is out of school
- If an educationally valuable website is blocked, students should contact their teachers to request the site be unblocked
- Anyone using a Cornerstone Chromebook, laptop or other network system has no expectation of privacy in such use. The District has the right to, and does, monitor use of these systems.
- Teachers, school administrators and the technology department may use monitoring software that allows them to view the screens and activity on a student device. This allows the teachers to review student classwork and school officials to ensure student safety.

CORNERSTONE
SCHOOLS

5.0 CONDUCT REQUIRING DISCIPLINARY ACTION

As mentioned throughout this document, misuse of Chromebooks has the potential to earn disciplinary consequences such as, but not limited to, lunch detentions, in school detentions, In School Suspensions, and Out of School Suspensions. Examples of conduct warranting disciplinary action include, but are not limited to the following:

- Leaving Chromebook unattended or an unsupervised area
- Failure to utilize protective case
- Inadequate care for Chromebook, case, charger, and other peripherals
- Multiple damage instances caused by abuse or neglect of Chromebooks and peripherals
- Resetting Chromebook to factory defaults
- Placing the Chromebook in developer mode
- Removal of MSE Asset Tags
- Downloading inappropriate apps and media
- Using the device to engage in inappropriate behaviors
- Adjusting songs on someone else's Chromebook
- Deleting school-installed settings from a Chromebook
- Adding a credit card to a Google Account (Google Wallet) to purchase music/unapproved apps
- Leaving Chromebook at home; lack of preparation for classes
- Repeatedly bringing uncharged Chromebooks to school
- Bringing Chromebook to Phys. Ed. class, unless directed to by P.E. teacher
- Loaning of student device to other students inside and outside of school
- Using a personal Google account to download purchased apps for yourself or another student(s)
- Using a program to bypass MSE Network Security, including web and content filtering
- Using a program to gain access to other students' accounts
- Illegal installation of transmission of copyrighted materials
- Transmission or accessing materials that are obscene, offensive, threatening or otherwise intended to harass or demean recipients
- Non-compliance of District policies. Failure to comply with the guidelines listed in this Handbook, or repeated occurrences of Chromebook damages caused by neglect or abuse, may result in the further disciplinary action, fees, and the loss of home use privileges.

I.   **PARENT/GUARDIAN RESPONSIBILITIES**

Before a device can be issued to students for school and home use, parents/students must sign this document. Parents are encouraged to provide a safe environment for students to use their Chromebooks at home for school assignments. Parents/Guardians are also encouraged to:

- Set rules for student use at home.
- Allow use in common areas of the home where student use can easily be monitored.
- Demonstrate a genuine interest in student's use of devices.
- Reinforce the idea that the device is a productivity tool to support learning, rather than used as a form of entertainment.

II.   Consequences for Violation of Technology Policies

Violation of the school's policies and procedures concerning the use of the computer on the network will result in the same disciplinary actions that would result from similar violations in other areas of school policy, including the Student Code of Conduct.

Use of the computer network and Internet is an integral part of research and class work, but abuse of this technology can result in loss of privileges. Students who use technology devices, digital resources, and network infrastructure, along with information technology inappropriately may lose their access privileges and may face additional disciplinary or legal action.

The length of time for loss of privileges will be determined by building administrators and/or other staff members. If the user is guilty of multiple violations, privileges can be removed for one year or more. Any or all of the following consequences may be enforced if a student violates the terms of this policy:

1. **Verbal/Written Warning:** The teacher may issue a verbal or written warning to the student for minor infractions or first-time offenses. This serves as a reminder of the rules and expectations.

2. **Temporary Loss of Privileges:** If a student repeatedly violates the Chromebook rules, they may face temporary loss of Chromebook privileges. This means they may be required to use alternative methods for completing assignments or may have restricted access to certain online resources. If the device is forgotten at home or not charged when bringing it to school, and it

happens 3 more times, the device will have to be left at school and will result in the consequence of losing the privilege to take the device home.

3. **Detention or After-School Work:** In more severe cases, students may be assigned detention or required to stay after school to complete additional work as a consequence for misusing their Chromebooks.

4. **Parental Notification:** The school may contact the parents or guardians to inform them about the student's inappropriate behavior or repeated violations of Chromebook policies.

5. **Loss of Chromebook Privileges:** For serious or repeated offenses, the student may lose their Chromebook privileges for an extended period. This means they may be required to use alternative means for completing assignments and may not have access to the Chromebook during class. (Note: Loss of computer privileges/Internet access, with a length of time to be determined by campus administration.)

6. **Disciplinary Action:** In extreme cases, where the student's actions significantly disrupt the learning environment or involve severe violations, disciplinary action may be taken. This can include suspension or other measures in accordance with the school's disciplinary policies. Suspension may be considered for flagrant violations or violations that corrupt the educational value of the computers or the Internet. Expulsion may be considered in instances where students have used the school's Internet access to engage in conduct that constitutes felony criminal mischief, and/or have deliberately attempted to bypass installed security software or copy/modify another student's work files.

6.0 TERMS OF USE

Cornerstone Schools reserve the right to deny, revoke or suspend specific user privileges and/or take other disciplinary action, including suspensions or expulsion from school, for violations of this policy. District and technology administration reserves the right to examine, use and disclose any data found in the district network and/or equipment in order to further the health, safety, discipline or security of the school community. Additionally, all handbook regulations apply to the use of the district network, internet and electronic resources.

7.0 DISCLAIMER

Cornerstone Schools, its employees and agents, make no warranties of any kind, neither expressed nor implied, concerning the network, internet access and electronic resources it is providing.

Furthermore, the school is not responsible for:

1. The accuracy, nature, quality, or privacy of information stored on local servers or devices or information gathered through Internet access.

2. Any damages suffered by a user (whether the cause is accidental or not) including but not limited to, loss of data, delays or interruptions in service, and the infection of viruses or other malware on personal computers or other devices.

3. Unauthorized financial obligations resulting from the use of Cornerstone Schools electronic resources.

Cornerstone Technology User Authorization

I hereby certify that I have read and understand Cornerstone Schools Student Acceptable Use Policy and agree to abide by its terms and conditions. I understand that if I violate the Student Acceptable Use Policy, my network/Internet access privilege will be revoked, and I will be subject to disciplinary action. I further understand that a violation of the Student Acceptable Use Policy may subject me to criminal and/or civil liability.

Student Name / Signature: *SIGN FORM ON POWERSCHOOL*

Parent or Guardian Name / Signature: *SIGN FORM ON POWERSCHOOL*

As the parent or guardian of the above-named user, I hereby certify that I have read and understand Cornerstone Schools Student Acceptable Use Policy.

I further understand that some materials accessible to network/Internet users may be offensive, illegal, defamatory or inaccurate, and that although the Cornerstone Schools has taken reasonable precautions to restrict access to such materials, such exposure may nevertheless occur. With that understanding, I hereby give permission to the Cornerstone Schools to allow internet access for my child. I further agree to indemnify and hold harmless Cornerstone Schools, its employees and agents from any and all claims arising from or related to my child's use or misuse of the computer equipment/Internet, and waive any and all claims I may have against Cornerstone Schools for such use or misuse.

Cornerstone Schools provides equipment for educational use. Individuals utilizing district provided equipment agree to the following statements:

As a student, I will:

- Use school technologies for school-related activities.
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline. Be courteous and respectful.

- Not post any information that I would not want students, parents, teachers, or future colleges or employers to see (once something is online, it is available to the world).
- Treat school resources carefully, and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, and posts) online.
- Use school technologies at appropriate times and in approved places, for educational pursuits.
  - Cite sources when using online sites and resources for research.
  - Recognize that use of school technologies is a privilege and treat it as such.
  - Be cautious to protect the safety of others and myself.
  - Help to protect the security of school resources.

As a student, I will not:

- Use school technologies in a way that could be personally or physically harmful.
- Attempt to find inappropriate images or content; intent to seek inappropriate images or content is a violation of this Acceptable Use Of Technology Policy.
- Access or participate in chats, chat rooms or instant messaging services on school computers unless authorized by a staff member for legitimate educational purposes
- Create a personal mobile "hot-spot" or utilize a "proxy site" for the purpose of circumventing network safety measures and filtering tools.
- Create, distribute or deploy multi-user servers or gaming software on any school devices.
- Use the district network system for commercial purposes. This means that students may not offer, provide or purchase products or services through the system.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- Try to find ways to circumvent the school's safety measures and filtering tools; intent to circumvent safety measures and filtering tools is a violation of this Acceptable Use Of Technology Policy.
- Use school technologies to send spam, chain mail or social media threats.
- Airdrop or send lewd messages or images to other students' mobile devices.
- Plagiarize content I find online.

- Post or otherwise disclose personally identifying information, about others or myself.
  - Agree to meet someone I meet online in real life.
  - Use language online that would be unacceptable in the classroom.
  - Use school technologies for illegal activities or to pursue information on such activities.
- Attempt to hack or access sites, servers, or content that isn't intended for my use.
- This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Student Name / Signature: *SIGN FORM ON POWERSCHOOL*

Parent or Guardian Name / Signature: *SIGN FORM ON POWERSCHOOL*

* PARENT / GUARDIAN <u>AND</u> STUDENT MUST SIGN *