CLOVER

CONNECTED CLASSROOM

Mobile Computing Guide

Last Edited Summer 2021

Welcome to Clover's Connected Classroom!

Our Connected Classroom outcomes include:

Creativity	because we value meaningful experiences that shape students' vision for the future and these will foster creativity.
Collaboration	because we value continuous improvement through collaboration. Our devices will connect us to vast resources, including people with whom we can collaborate.
Problem Solving	because we value an individualized and personally relevant education where students think critically and gain skills in problem solving. They will be able to apply learning in new situations.
Digital Citizens	because we value a safe and nurturing environment and will make every effort to build digital citizens who are prepared for a successful, productive and responsible future.

In 2012-13, Clover students had increased access to mobile computing devices via a cart model at each school. We already had multiple desktop and laptop labs in each building. In the 2013-14 school year, 33 classrooms were identified as Connected Classrooms where the students had constant access to assigned mobile computing devices. Elementary and middle school students in these selected classrooms had access to iPads while the selected high school teachers were using MacBook Airs. The computer labs and iPad carts remained in place for use by all students. For the 2014-15 school year and years to follow, the district has provided assigned mobile computing devices for all students whereby all classrooms would be Connected Classrooms.

Our Connected Classroom initiative is not about which digital tool is used. Rather, it is about the increased connectivity to people, places and things. It matters not which device students use to access information, but it matters that we have provided them both the tools and the instruction for use that they might be productive digital citizens. Our district mission is to prepare each child for a successful, productive and responsible future. Creating an engaging digital learning environment that doesn't know physical boundaries is key in accomplishing that mission. Providing devices to students connects them to limitless learning opportunities because they will have access to the most current information on any topic through the Internet and to our learning management system where they can communicate, collaborate, create, publish and learn. Teachers will be able to supplement printed resources and provide interactive applications to students like never before.

Table of Contents

Refer to the following website for all documents and forms mentioned in this guide and several other helpful resources: https://www.clover.k12.sc.us/connected

RECEIVING/RETURNING YOUR ASSIGNED MOBILE COMPUTING DEVICE

Distribution of Assigned Mobile Computing Devices

Students will be assigned a mobile computing device when they first enroll in the district. Assignments will be verified each new school year.

Resources for parents that address policies, procedures, and expectations can be found on the district website. Parents are expected to have reviewed this mobile computing guide when signing the acceptable use pledge each year.

The Technology Insurance Plan for Assigned Mobile Computing Devices offers families an option for protecting the Assigned Mobile Computing device. Please review the Technology Insurance Plan for Assigned Mobile Computing Devices included in this handbook (see Appendix A).

After a school issues an Assigned Mobile Computing device to a student for take home or day use, parents/guardians must accept and sign the Technology Insurance Plan for Assigned Mobile Computing Devices and Student Pledge documents (see Appendices A & B) within the first month of attendance.

Daily Use Protocols: Take Home versus Day Users

Take home users are able to use their devices at school as well as home. To be eligible to be a take home user, students/parents must have signed the Technology Insurance Plan (see Appendix A) as well as the Student Pledge document (see Appendix B), and maintain responsible use of the devices.

Day users will have access to devices during the school day. They will check out their assigned devices each morning and back in after that school day ends. Students/parents must sign the acceptable use agreement.

Take home users may become temporary or permanent day users in the event that payments for repairs or replacements are not paid or if students have received disciplinary consequences for inappropriate use of a device. Status changes will be handled on a case by case basis.

Devices are issued for student use only. Inappropriate use by any other person outside of the district may result in disciplinary action for the student.

Assigned Mobile Computing Devices Left at Home

When students are given access to take the device home, it is the student's responsibility to bring the device back to school the following day fully charged. Students who leave their Assigned Mobile Computing devices at home are still responsible for completing their daily course work. Repeated offenses may result in disciplinary action.

Assigned Mobile Computing Devices Undergoing Repair

The school may issue a loaner Assigned Mobile Computing device to a student while his/her Assigned Mobile Computing device is being repaired. A student may not receive a loaner immediately. There may be a delay depending upon availability of a loaner Assigned Mobile Computing device and quickness of repair process. If fees for damages or replacement are issued for the student to pay, the student will remain a day user until the balance becomes zero and required paperwork is returned.

Returning Assigned Mobile Computing Device

Students leaving Clover School District during the school year must return the Assigned Mobile Computing device (including MacBook power cords, cases and any other district- or school-issued accessories). Likewise, graduating seniors will return their Assigned Mobile Computing devices (including power cords, cases and any other district- or school-issued accessories) before graduation. If a student does not return his/her Assigned Mobile Computing device upon leaving the district, the student will be subject to criminal prosecution or civil liability. The student will also be required to pay the replacement cost for a new Assigned Mobile Computing device if one is not returned.

If a student returns his/her Assigned Mobile Computing device that has been damaged, costs for replacement or repairs are the student's responsibility. The district will charge the student the cost of needed repairs, not to exceed the replacement cost of the Assigned Mobile Computing device. If a student is covered under the Technology Insurance Plan, repairs are covered unless the damage is due to negligent/malicious behavior, in which case the student will pay for the repair or replacement.

Identification of Assigned Mobile Computing Device

Each student's Assigned Mobile Computing device will be labeled in the manner specified by the district. Assigned Mobile Computing devices can be identified by Serial Number and/or MAC address as well as by a Clover School District Asset Tag. Name barcodes and asset tags should not be removed or obstructed at any time.

CARING FOR THE ASSIGNED MOBILE COMPUTING DEVICE

The Assigned Mobile Computing device is district property. All users will follow these guidelines and the Clover School District Acceptable Use of Technology policy (IJNDB and IJNDB-R in Appendix C).

Students are responsible for device protection when it is in their possession. Students will report loss, malfunction or damage to a staff member immediately. School staff members will report lost, malfunctioning, or damaged devices immediately to the technology staff for evaluation and/or repair.

General Precautions

Use only a clean, soft cloth to clean the screen. Do not use cleansers of any type.

Carefully insert or remove cords and cables into the Assigned Mobile Computing device to prevent damage.

Devices must remain in their district-issued cases at all times with identifying labels in tact and unobstructed.

Devices should only be changed using Apple-approved charging cables.

Never leave your Assigned Mobile Computing device visible in a parked vehicle or any other unsupervised area.

Screen damage will occur when excessive pressure is applied to the screen. Users must avoid leaning on the top of the device or placing objects in a book bag or protective case in a way that will apply pressure to the screen.

Do not bump the Assigned Mobile Computing device against lockers, walls, car doors, floors, etc., as it will crack/break the screen.

Carrying Assigned Mobile Computing Devices

The district provides students with protective cases for their Assigned Mobile Computing devices. These cases provide sufficient protection for typical use.

Students must keep their Assigned Mobile Computing devices inside the protective cases at all times. Cases should not hold other objects. When placing a device in a backpack, care should be given to avoid applying excessive pressure and weight on the Assigned Mobile Computing device screen.

Assigned Mobile Computing device protective cases furnished by the school district must be returned with only normal wear and no alterations to avoid a case replacement fee.

USING YOUR ASSIGNED MOBILE COMPUTING DEVICE

Assigned Mobile Computing devices are intended for use at school. In addition to teacher expectations for device use, students may access school messages, announcements, calendars and schedules using their Assigned Mobile Computing device.

Printing

Students can print from their Assigned Mobile Computing devices when given permission to do so. Schools will give students information about printing with the Assigned Mobile Computing devices while at school.

School Internet Access

The district provides filtered Internet access on campus. Students are prohibited from downloading unauthorized content (ie. applications, proxy servers, music, VPNs, etc.) to a district-issued mobile device. Attempts to circumvent district filtering will lead to disciplinary consequences.

Home Internet Access

Students may establish Wi-Fi connections with their Assigned Mobile Computing devices outside of school. Students can then use the mobile computing device wherever access is available. Clover School District can not guarantee filtered Internet access off campus.

Camera Use

The Assigned Mobile Computing device comes equipped with photo and video capabilities.

The Family Educational Rights and Privacy Act (FERPA) is a federal law that affords parents and students over 18 years of age certain rights with respect to students' educational records including photographs. You can read more about FERPA in the Forms and Notices packet you received at the beginning of school and/or online at http://www.clover.k12.sc.us//site/default.aspx?PageID=4311.

For this reason, students must obtain permission to publish or make publicly available a photograph or video of any school-related activity. Unauthorized recordings are subject to disciplinary action in accordance with the district's Acceptable Use Policy (see Appendix C).

Clover School District retains the rights to any recording and/or publishing of any student or staff member's work or image.

MANAGING YOUR FILES AND SAVING YOUR WORK

Saving to the Cloud

It is recommended that students save their work in the cloud and share files or folders with other students and/or their teacher(s). Files are assigned to the student until the student shares them with another user. Clover School District retains the rights to any recording and/or publishing of any student or staff member's files or folders stored within a school-assigned cloud.

It is each student's responsibility to ensure that his/her work is not lost due to mechanical failure or accidental deletion. Students should regularly back their devices up to the cloud.

Assigned Mobile Computing device malfunctions are not an acceptable excuse for failure to submit work.

Network Connectivity

Clover School District makes no assurance that the network will be operational at all times. The district will not be responsible for lost or missing data. Check the status of district services at https://status.clover.k12.sc.us/.

APPLICATIONS ON ASSIGNED MOBILE COMPUTING DEVICES

The applications originally installed by Clover School District on each Assigned Mobile Computing device must remain on the Assigned Mobile Computing device in usable condition and readily accessible at all times.

Some licenses for applications require that the application be deleted from the Assigned Mobile Computing device at the completion of a course.

The district will distribute upgraded versions of licensed applications from time to time through network processes or manually by a technician.

Teachers may direct students to load additional applications on their Assigned Mobile Computing devices from the district provided app repository.

If technical difficulties occur or unauthorized applications are discovered, technology staff will restore the Assigned Mobile Computing device. The technology staff does not accept responsibility for the loss of applications or documents deleted due to a restore to factory default.

DIGITAL CITIZENSHIP

Digital Citizenship is a concept that helps students understand how to use technology appropriately in a digital society.

The district expects students to use technology appropriately and responsibly whether in electronic communication or participation.

The district has electronic precautions in place in order for students to participate safely and securely in this environment and enjoy the rights of a digital world in an educational setting.

Annually, Clover School District delivers essential lessons to all students to remind them about responsible use. Throughout the year, students receive instruction about various digital tools.

District and Teacher Responsibilities

The district will provide Internet and email access to students while on school properties. Filtering/blocking of inappropriate Internet materials while on district campuses is done at the district level.

The district provides cloud-based storage for all students.

School staff will help students conduct research and ensure student compliance with the district's Acceptable Use Policy (see Appendix C).

Clover School District reserves the right to investigate any inappropriate use of resources and to review, monitor, and restrict information stored on or transmitted via Clover School District-owned equipment and resources and take appropriate action.

Student Responsibilities

Students will abide by the district's Acceptable Use Policy (see Appendix C) and:

- contact an administrator about any security issue they encounter.
- monitor all activity on their assigned account(s).
- keep the device updated and backed up to the cloud.
- report communication containing inappropriate or abusive language or questionable subject matter to a teacher or administrator.
- return their Assigned Mobile Computing device to the issuing school on or before the date they withdraw, graduate, or transfer to another school district.

Parent/Guardian Responsibilities

Parents/guardians are encouraged to review policies, procedures and expectations.

All district-issued Assigned Mobile Computing devices do not contain a filter for use at home. Parents/Guardians are expected to monitor student activity at home, especially Internet access.

Devices are for student-use. The proper use and content of the device is the responsibility of the student regardless of whether another user outside of the district may have accessed the device. Disciplinary action will be taken if inappropriate content is found on the device regardless of whether it was accessed at school or at home.

Talk to your children about the values and standards you expect them to follow as they use the Internet just as you talk to them about their use of all other media information sources, such as television, telephone, movies, radio, etc. You can find a variety of helpful resources for sharing age-appropriate concepts with your children at the following website: http://www.commonsensemedia.org.

Creative Commons Copyright

At a teacher's discretion, student work may be uploaded to the Internet.

While the student's original works are his/her intellectual property, the district owns the copyright to the products generated on district-owned devices. Students are encouraged to select one of the Creative Commons Copyright licenses to include with their work. This license will state how the work can be used by others.

ASSIGNED MOBILE COMPUTING DEVICE DAMAGE OR LOSS

Terms of the Assigned Mobile Computing Device Agreement

Terms and conditions that apply to the usage of the Assigned Mobile Computing Device under the Technology Insurance Plan are as follows:

- The district provides access to the Technology Insurance Plan (see Appendix A) for all issued devices at no charge at the beginning of each school year to cover one accidental damage claim.
- The Technology Insurance Plan covers parts and repair for system-related issues or failures occurring from normal use. It does not cover damages resulting from negligent or malicious behavior. Special circumstances may be addressed at the discretion of building administration. It also does not cover the repair or replacement of charging cables, protective cases, iPad keyboards and other accessories.
- The Technology Insurance Plan covers **one** of the following:
    - ☐ Repair of one accidentally broken device
    - ☐ Repair of damages resulting from normal use
    - ☐ One device replacement in the event of a catastrophic loss
    - ☐ One device replacement in the event of theft
- In the event an Assigned Mobile Computing device covered by the Technology Insurance Plan is stolen, the student or parent/guardian must report the theft to the school and file a police report within 48 hours in order to avoid paying the cost to replace the device.
- In the event an Assigned Mobile Computing device covered by the Technology Insurance Plan is lost, the student or parent/guardian must either recover the device or file a police report within 5 days. On the sixth day, the school will begin actively pursuing the device. On the tenth day, the school will file a police report for the missing device. Parent/guardian(s) may be listed as suspects in the report.
- Families are given the option to renew the Technology Insurance Plan after its use for $25 fee per incident.

- Students must comply at all times with Clover School District's Assigned Mobile Computing Device Agreement (see Appendix A). Failure to comply ends the right of possession effective immediately.

Title, Possession and Liability

Legal title to the property is with the district and shall at all times remain with the district. The right of possession and use is limited to and conditioned on full and complete compliance with the Assigned Mobile Computing Device Agreement. Failure to comply will result in device repossession.

The student is responsible at all times for the Assigned Mobile Computing device's appropriate care and use.

Clover School District reserves the right to require the return of the Assigned Mobile Computing device at any time. Assigned Mobile Computing device agreements are good for one year (from the first day of school in the current school year until the last day of summer as defined on the district calendar), unless the agreement is terminated earlier.

Failure to return the Assigned Mobile Computing device to the issuing school before departure from the district may result in criminal charges brought against the student and/or the person in possession of the Assigned Mobile Computing device.

Damages Resulting from Negligent/Malicious Behavior

Students are responsible for the entire cost of repairs to an Assigned Mobile Computing device they intentionally misuse, abuse or damage. Investigations are completed by building administration and circumstances will be considered on a case by case basis. Students will become day users until balances for repair or replacement are paid in full.

Estimated Repair Pricing for Repeated or Malicious Damage or Neglect:

iPad

All iPad repairs are handled by the Apple Care program. Damages not covered under Apple Care result in full replacement cost of the device. Apple Care coverage is determined solely by the Apple Care Team.

Costs that are not ever covered by the TIP:

- Logitech Crayon — $50
- Apple Pencil — $120
- Case — $25

MacBook Air

Possible repairs include: Keyboard, Trackpad, LCD screen, System board, Battery, or Hard Disk Drive. The costs for these could range from $100 to $800 and will be determined by Apple.

Costs that are not ever covered by the TIP:

- Power adapter and cord — $80
- Case — $35

If a student is found to have intentionally stolen or damaged a device and the device cannot be retrieved or repaired, he/she will be charged fair market value for a replacement.

iPad	**MacBook Air**
1 year old device 100% of replacement cost	1 year old device 100% of replacement cost
2 year old device 66% of replacement cost	2 year old device 75% of replacement cost
3 year old device 33% of replacement cost	3 year old device 50% of replacement cost
	4 year old device 25% of replacement cost

Unintentional Loss or Theft

Students are responsible for the Assigned Mobile Computing devices assigned to them. Tips to avoid loss/theft of the device:

- Never leave an electronic device unattended in a public place.
- Secure electronic items in a vehicle out of sight, preferably locked in a trunk when the car is unattended.
- Leave devices at school or home when they are not being used for school related work.

In the event of loss or theft, appropriate actions are given below.

In the event of accidental loss:

In the event an Assigned Mobile Computing device is lost, the student or parent/guardian must report the loss to the school immediately. The student or parent/guardian must either recover the device or file a police report within 5 days. On the sixth day, the school will begin actively pursuing the device. On the tenth day, the school will file a police report for the missing device. Parent/guardian(s) may be listed as suspects in the report. Without a recovered device or completed report, parent/guardian(s) will have to pay fair market value for the device. Students will become day users until the full balance is paid. In the event the device is recovered, the replacement costs paid to date will be refunded.

In the event of catastrophic loss:

In the event an Assigned Mobile Computing device is lost or damaged beyond repair by an act of nature or man beyond control, the student or parent/guardian must report the loss to the school immediately. Examples include but are not limited to a fire or automobile accident. Once the event is confirmed, the student will be assigned a new device. This cost is may be covered by the student's TIP if available or the parent/guardian would be responsible.

In the event of theft or vandalism on campus:

In the event an Assigned Mobile Computing device is stolen, vandalized, etc., the student or parent/guardian must report the event to the school and file a police report within 48 hours. Students or parent/guardians must file a police report with the school resource officer when incidents occur on campus. Once the incident has been confirmed, a new device will be issued

to the student. This cost is may be covered by the student's TIP if available or the parent/guardian would be responsible.

In the event of theft or vandalism off campus:

In the event an Assigned Mobile Computing device is stolen, vandalized, etc., the student or parent/guardian must report the theft to the school and file a police report within 48 hours. Students or parent/guardians must file a police report with local law enforcement within 48 hours when incidents occur off campus and provide a copy of the completed police report to the school. Once incident has been confirmed, a new device will be issued to the student. This cost is may be covered by the student's TIP if available or the parent/guardian would be responsible.

The procedures for determining the type of loss and course of action include:

1. Personal meeting with student and administrator to investigate the event
2. Personal call or meeting with administrator and parent
3. Determination when and how a new device can be issued to a student

APPENDIX A: ASSIGNED MOBILE COMPUTING DEVICE AGREEMENT

Technology Insurance Plan for Assigned Mobile Computing Devices - School Year 2020-2021

The Technology Insurance Plan was design to help sustain the investment Clover School District has made in mobile computing devices.

Terms of the Technology Insurance Plan for Assigned Mobile Computing Devices

The district provides access to the Technology Insurance Plan for all issued devices at no charge at the beginning of each school year to cover one accidental damage claim. The Technology Insurance Plan covers parts and repair for system-related issues or failures occurring from normal use. The plan includes the repair/replacement of one Assigned Mobile Computing device per school year in the event of theft, accidental damage, or catastrophic loss.

Any-fees resulting from damages not covered by the Plan will be the responsibility of the student/parent/guardian. The cost of repair or replacement will not exceed the Fair Market Value of an Assigned Mobile Computing device. Parents/Guardians must report lost or stolen devices as outlined in the Mobile Computing Guide.

After initial use of the Technology Insurance Plan, it may be renewed for a $25 fee per incident.

Damages/Loss Not Covered by Technology Insurance Plan

The Technology Insurance Plan **does not** cover the repair or replacement of charging cables, protective cases, iPad keyboards and other accessories. Students will be responsible for the entire cost of replacement or repair for Assigned Mobile Computing device damages due to negligent or malicious behavior. Special circumstances may be addressed at the discretion of building administration.

Technology Insurance Plan for Assigned Mobile Computing Devices - School Year

I understand and agree to the terms of the Technology Insurance Plan.

Student Name (Please Print): _____

Parent/Guardian Name (Please Print): _____

Parent/Guardian Signature: _____ Date: _____

APPENDIX B: STUDENT PLEDGE FOR ACCEPTABLE USE OF AN ASSIGNED MOBILE COMPUTING DEVICE

The district will provide students with access to the Internet, an assigned mobile computing device ("device"), and a variety of applications to enhance student learning within the classrooms using technology. Technology is to be used in a responsible, efficient, ethical and legal manner. In order to participate in the use of technology, all students must agree to abide by the generally accepted rules of use found in the following statements.

1. I will use technology as a learning tool and understand that it can greatly enhance my ability to be an independent learner.

2. I will be responsible and accountable for the device(s) assigned for my use and will take proper care of this device as follows.

    a. I will only use the devices assigned to me and will bring it to school daily with a fully charged battery.
    b. I will not loan the device or charger and cords to others.
    c. I will protect mobile devices by keeping them in the case at all times.
    d. I will not stack objects on top of the device.
    e. I will immediately report any damage or issues to my teacher.
    f. I will not disassemble any part of the device nor attempt repairs.
    g. I will keep food and beverages away from the device.
    h. I will not leave the device unattended.
    i. I will report a lost device immediately to a school employee.
    j. I will file a police report within 48 hours in case of theft or vandalism.

3. I will not download unauthorized content (ie. applications, proxy servers, music, VPNs, etc.) to a mobile device.

4. I will not use messaging or other social tools during school hours unless instructed. I will remember that electronic messaging (including mail or in-app messaging) is not guaranteed to be private. The district system administrator has access to all electronic messages. Messages relating to or in support of illegal or inappropriate activities will be reported to the appropriate authorities.

5. I will always use appropriate language. Abusive, profane, vulgar and other inappropriate language is prohibited.

6. I will never reveal my assigned address or phone number or that of others.

7. I will ensure my behavior on the Internet or use of technology does not disrupt, harass or annoy other users.

8. I will always cite all quotes, references and sources, and I will not use another person's material as my own.

9. I will never access inappropriate or restricted information or other information not directly related to the educational purposes for which access is being provided. Restricted information includes obscene,

libelous, indecent, vulgar, profane or lewd materials and advertisements for products or services not permitted to minors by law.

10. I will never purposefully harm hardware or destroy or tamper with data of another user. Vandalism is prohibited and includes, but is not limited to, the uploading or creation of computer viruses.

11. I will not deface the serial number, manufacturer labels or district labels on any device. I will not place decorations (such as stickers, markings, etc.) on the device or district-issued protective case.

12. I will use the Internet only for research and academic purposes.

13. I will be responsible for backing up my content to a cloud storage device. At times, Clover School District will have to reset the device. All files not backed up will be deleted during these processes.

14. I will be responsible for all damage or loss caused by neglect or abuse.

15. I agree to return the device and school issued accessories in good working order.

I agree to the stipulations set forth in the Mobile Computing Guide and CSD Board Policies (IJNDB, IJNDB-R, JICJ, JICDA). I understand my Assigned Mobile Computing device is subject to inspection at anytime without notice and remains the property of Clover School District.

The district may impose disciplinary sanctions for off-campus behavior involving inappropriate use of the Internet. The posting of harassing, threatening or otherwise inappropriate comments on Internet websites is considered disruptive to school and may lead to disciplinary action. The use of the Internet is a privilege, not a right. Documented inappropriate use will result in the cancellation or restriction of Internet privileges.

Student's full name (print) _____

Student's signature _____

Date _____

As a parent/legal guardian of the student, I agree to review the rules listed above with my child and encourage safe, responsible use of technology. My child's signature indicates that he/she understands his/her responsibility in the care and use of technology.

Parent/Legal guardian permission _____

Parent/Legal guardian signature _____

Date _____

Board policy requires that an Acceptable Use Agreement be filled out annually in order for students to have access to the technology.

APPENDIX C: CLOVER SCHOOL DISTRICT ACCEPTABLE USE POLICY

IJNDB - Acceptable Use of Technology

Purpose: To establish the foundation for technology literacy for the students and employees of Clover School District.

By providing access to technology, the district intends to promote educational excellence in schools by facilitating resource sharing, innovation, communication and learning and by allowing access to resources unavailable through traditional means.

The availability of Internet access provides a unique educational opportunity for students and staff to contribute to the district's presence on the worldwide web. This medium of communication provides an opportunity to share accurate information with the community, the state and the world about the district's curriculum and instruction, school-authorized activities and other related information. The district provides this instructional resource as an educational tool for staff and the technology acceptable use policy will govern its uses. The failure to follow this policy may result in the loss of privileges or other disciplinary measures as outlined in JCDA.

The Clover School District has taken precautions to restrict access to inappropriate materials on the Internet. However, on a global network it is impossible to control all materials and a persistent user may discover inappropriate information. The school district believes that the valuable information and interaction available on this worldwide network far outweigh the possibility that users may procure materials that are not consistent with educational goals of the district. Users are responsible for reporting to the district's director of technology or his/her designee controversial or inappropriate websites they are able to access so the websites can be added to the district's filter.

In order to maintain access to the Internet, employees and students will abide by the rules and regulations for acceptable use outlined in administrative rule IJND-R. Unauthorized or inappropriate use of technology may include, but is not limited to: taking pictures or recording without permission, cheating, harassment or bullying, use during unauthorized times or use for unauthorized activities.

It is the purpose of this policy to establish basic rules for access/use of the Internet by students and employees in the Clover School District so that all use of this valuable resource is appropriate.

IJNDB-R - Acceptable Use of Technology

This administrative rule governs the use of the district's computers, network, Internet and electronic research and communication resources by district employees, students and guest users and the use of personal electronic devices used on school property or during school-related events. It is intended to protect the integrity of district operations and instructional programs, as well as to outline the rights and responsibilities of district employees and guest users. These rules will be in effect at all times.

Scope

This administrative rule applies to the following persons/entities.

- all district employees including regular, part-time, temporary and contract employees
- all students enrolled in district schools
- all other authorized users of any of the district's technology resources, regardless of district affiliation or reason for usage
- all district owned or operated technology resources or systems which are subscribed to and/or
- paid for by the district
- all personal electronic devices used on school property or during school-related events

Acceptable Use Agreements

At the beginning of each year, the principals will send letters to parents/legal guardians describing the level of Internet supervision and access available at the school. At the elementary grades, the teacher or technology assistant will directly control all Internet access. In grades 3-12, students will be required to read and sign the acceptable use contract, IJND-E(1). The contract must also be signed by the parent/legal guardian. Only those students with this signed contract on file will be allowed access to the Internet. Employees must sign a similar contract, IJND-E(2). These contracts spell out guidelines for Internet use as well as consequences for violating the guidelines.

Confidential information

The district's research, information and communication resource systems have security measures in place; however, such measures do not guarantee total security. As a result, information generally considered to be personal or confidential should not be sent via the district's communication resources except through means deployed for that purpose or approved for that purpose. The district cannot assume responsibility for lost or stolen information sent or received via the district's communication resources.

General digital technologies usage and online access

The following actions are prohibited.

- Knowingly loading or creating viruses

- Loading or attempting to load software or files onto a school computer without permission
- Loading or attempting to load software or files onto the district network without permission of the information technology department
- Accessing or modifying data without authorization
- Modifying passwords without authorization
- Unauthorized access, including so-called "hacking" or other unlawful activities
- Unauthorized disclosure, use or dissemination of personal information regarding minors

Network and Internet usage

Access to the district network and Internet is made available to authorized users for educational and district operational purposes. All authorized users will receive instruction on proper use of the district's network and Internet system. Although students will be under teacher supervision while on the network, it is not possible to constantly monitor every individual student and what data they are accessing on the network. Some students might encounter information that is not of educational value.

The district will not be liable for the users' inappropriate use of the district's electronic communication resources or violations of copyright restrictions, users' mistakes or negligence, or costs incurred by users. The district will not be responsible for ensuring the accuracy or usability of any information found on the Internet.

The district prohibits the use of its network and the Internet to intentionally access, view, download, store, transmit or receive any information that contains material which is in violation of any district policy or administrative rule, or any local, state and/or federal laws or regulations.

Prohibited material includes, but is not limited to, the following.

- Obscenity or pornography
- Threats
- Material that is intended, or could reasonably be perceived, to be harassing or discriminatory
- Inappropriate use of material that is copyrighted or protected by trade secret
- Material used to further any commercial business, product advertising, virus transmission or political activity
- Material that is potentially disruptive of the learning environment

The district reserves the right to monitor and/or review all uses of the district network and the Internet, and users should not have any expectation of privacy in any information accessed, viewed, downloaded, stored, transmitted or received.

Accessing inappropriate sites

The school district will use technology protection measures to the best of the district's ability to protect students from inappropriate access. Employee, student and visitor activities may be monitored by the district to detect unauthorized uses of the Internet and or access to inappropriate sites that have visual depictions that include obscenity, child pornography and other pornography or otherwise are violations of this administrative rule.

Reporting

District and school computer technicians as well as other district employees who are working with a computer and come across sexually explicit images of children must report this to local law enforcement. The report must include the name and address of the owner or person in possession of the computer.

Off-campus conduct

Students, parents/legal guardians, teachers and staff members should be aware that the district may take disciplinary actions for conduct initiated and/or created off-campus involving the inappropriate use of the Internet or web-based resources if such conduct poses a threat or substantially interferes with or disrupts the work and discipline of the schools, including discipline for student harassment and bullying.

Personal use of social media

When staff members or students publish content, post pictures or maintain dialogue through Facebook or any other social networking tool, the professionalism, integrity and ethics in their role as an educator or student should never be compromised.

A Facebook fan page may not be used to replace a school or class website. A Facebook fan page is limited to extracurricular activities and clubs outside of the regular classroom. Staff members who want to use fan pages for student groups must have approval from the building administrator and from the district.

Inappropriate use of social media or electronic communication tools may result in disciplinary action up to and including dismissal.

Electronic mail (email) usage

The district's email system is made available to authorized users for educational and district operational purposes. All authorized users will receive instruction on proper use of the district email system.

The district prohibits the use of its email system for unprofessional and/or inappropriate purposes to include, but not be limited to, the following.

- Creating, transmitting or receiving emails containing any language or depictions that could reasonably be perceived by others as being offensive, threatening, obscene, sexual, racist or discriminatory
- Any use that violates local, state and/or federal laws or regulations
- Setting up or operating a commercial business

All electronic messages created, transmitted or received via the district's email system, including those created, transmitted or received for personal use, are the property of the district. The district reserves

the right to archive, monitor and/or review all use of its email system and users should not have any expectation of privacy in any electronic message created, transmitted or received on the district's email system.

Handheld communication device usage

District-issued cell phones or other handheld communication devices are to be used only by the employee to whom the phone or communication device was issued and are to be used only for matters directly related to the employee's job responsibilities. The district reserves the right to monitor and/or review all use of district-issued phones and communication devices and users should not have any expectation of privacy in any use of a district-issued phone or communication device.

Personal use of district research, information and communication resources

Limited personal use of district computers, the district network and the Internet and electronic research and communication resources is permitted to the extent that such use does not disrupt or interfere with the operation of the district and its instructional programs. Excessive personal use that may or does so disrupt or interfere is prohibited.

Third party access to systems and/or data

Within limited circumstances, the district sub-contracts specific work to be performed on behalf of the district in areas including, but not limited to, software development, system support, hardware acquisition and provisioning, and training. As part of these agreements, specific authority is granted to the sub-contracted third party to access the district's network and data, including student information and financial information. These agreements and authorizations of access to systems, networks or data are temporary in duration and bound by non-disclosure principles, confidentiality and time frames established within the agreement between the district and any third party. All local, state and federal statutes, laws or regulations regarding confidentiality of student information or financial information apply.

Sub-contracted work being performed on behalf of the district is limited to the specified parameters within the agreement. Upon completion of the agreed upon work, access to district systems or data is to be considered terminated. This termination of access will be accomplished either by manual action taken by the district technology department, or considered as the default access status of the third party following the completion of agreed upon work or tasks.

At no time will access to systems or data be continued beyond the completion of work or duration of specified time. Any physical or virtual access, either locally or remotely, to networks, systems or data must be approved by the district technology department or the superintendent. No other district entity holds the authority to grant access to any networks, systems or data. In circumstances where access is granted, the specific access is valid only for the duration of specifically agreed upon work and/or time frames. At the completion of agreed upon work, access is considered terminated. Once access is considered terminated, new authorization of access must be granted by the district technology department or the superintendent prior to any new work, continuance of work or attempted access. Continuance of access authority is never automatic or to be assumed by any third party.

Violations

All authorized users of district research and communication resources are expected to report any use that is believed to be unauthorized, excessive or otherwise in violation of this administrative rule. District employees who witness, experience or otherwise learn about a suspected violation should report the matter to their immediate supervisor. Students who witness, experience or otherwise learn about a suspected violation should report the matter to a teacher or school administrator. Other authorized users who witness, experience or otherwise learn about a suspected violation should report the matter to a district administrator.

An employee's personal use of non-district issued electronic communications resources outside of working hours will be the concern of, and warrant the attention of, the board if it impairs the employee's ability to effectively perform his/her job responsibilities or as it violates local, state, or federal law, or contractual agreements (see policy GBEB regarding use of non-district issued electronic resources).

All suspected violations will be investigated thoroughly. If it is determined that a violation of this administrative rule has occurred, the following disciplinary and/or corrective actions may be taken.

- Review of and possible changes to the level of supervision and the circumstances under which use is allowed
- Limitation, suspension and/or termination of the violator's user privileges
- Disciplinary measures determined to be appropriate based on the seriousness of the violation, up to and including termination or expulsion
- Report to law enforcement when the violation is believed to constitute a violation of a state or federal law or regulation

JICJ – Use of Personal Electronic Devices in School

Purpose: To establish the basic rules for the board's permission of student use of cell phones and other personal electronic devices in schools.

For purposes of this policy, a personal electronic device includes, but is not limited to: cell phones, pagers, gaming devices, or other devices that emit an audible signal, vibrate, display a message, display or record an image, or otherwise summon or deliver a communication to the possessor. Students may possess a cell phone or other personal electronic device in school, as long as it is used during authorized times and is not disruptive to the educational environment.

Unauthorized use of a cell phone or other personal electronic device may include, but is not limited to: taking pictures or recording without permission, cheating, harassment or bullying, use during any emergency drill, use during unauthorized times or use for unlawful activities.

Parents/legal guardians are advised that the best way to get in touch with their child during the school day is by calling the school office. Students may use school phones to contact parents/legal guardians during the school day with permission of the administration.

Students, parents/legal guardians, teachers and staff members should be aware that the district may take disciplinary action against students consistent with policy JICDA/JICDA-R regarding student conduct.

Elementary school

Elementary students may not use or display cellular phones, beepers and pagers while on school property during school hours. (The start and end of school will be denoted by the start and end bell.)

Middle school and High school

Middle school and high school students may use ECDs such as cellular phones, electronic pagers or any other communications devices before and after school, during their lunch break, within "free zones" as determined by the principal, and/or for educational and/or instructional purposes only as deemed appropriate by the teacher and approved by the principal. Any other use of wireless communications is considered misuse and violations may result in disciplinary action.

Consequences for inappropriate use may include, but are not limited to:

- warning/confiscate device and return to student at the end of the school day
- confiscate device/return to parent/legal guardian
- confiscate device/return device to parent/legal guardian and privilege to have device is revoked for the remainder of the school year
- confiscate device/return at the end of the school year

Possession of a personal electronic device on school property acknowledges consent to search the contents of the device in a school or criminal investigation. In such investigations, students will provide necessary login information as needed.

A student in possession of a cell phone, or other personal electronic device in conflict with this policy will be subject to discipline as provided under the District's code of student conduct (policy JCDA/ JCDA-R).

APPENDIX D: CLOVER SCHOOL DISTRICT ASSIGNED MOBILE COMPUTING DEVICE DISCIPLINE PLAN

Schools have further defined the consequences for various violations, but all fit within the guidelines below.

Level 1 Violations

Include but are not limited to: repeated uncharged device, unprepared for class, careless or irresponsible use, off task behavior

1st offense – teacher-based discipline
2nd offense – teacher-based discipline
3rd offense – teacher-based discipline with parent contact
4th offense – refer to administration

Examples of teacher-based discipline include:

- verbal redirection
- student/teacher conference
- restricted use in the classroom
- alternate assignments
- teacher assigned detention
- parent/teacher communication/conference

Level 2 Violations

Include but are not limited to: acceptable use policy violations, photographing/filming others without permission or against their will, bullying with the device, harmful or malicious activities, accessing and/or sharing inappropriate websites, materials, videos or photos

Examples of administrator discipline include:

- Student/administrator conference
- Restricted use of device/restricted user
- In-School Suspension (1-5 days)
- Out of School Suspension (1-5 days)

Any offense classified as level 2, a major classroom disruption, or criminal conduct will be referred immediately to an administrator and/or the School Resource Officer. The administrator will notify parents and determine discipline. Only an administrator can assign ISS or OSS.

Level 3 Violations

Include criminal offenses that require the involvement of law enforcement and may require arrest and/or a recommendation for expulsion.

Possession and use of personal and/or school issued electronic devices on school property acknowledges consent to search the contents of the device in a school or criminal investigation. In such investigations, students will provide necessary login information as needed. Misuse of technology outside of school that impacts the people or environment on campus may also necessitate similar disciplinary consequences and searches.

The administration reserves the right to handle any of the above actions or any other action determined to be a misuse of technology in the manner they feel is the most appropriate for all concerned. For additional information on acceptable use of technology, please refer to the CSD Technology Acceptable Use Policy.