Dyersburg Middle School
Chromebook Responsible Use Policy, Procedures and Information Guide

Jeremy Hinson
Principal

DMS Chromebook Assigned to Me:

Name: _____.

Number of the Chromebook: _____.

Serial #: _____.

Table of Contents

What happens if the device is damaged or lost?
Students and parents will be responsible for school-owned technology property that is issued to them, just as they are for other school-owned items such as textbooks, calculators, cameras, athletics equipment or library books. The district will repair or replace the device, but students and parents will be responsible for the cost of those repairs or replaced devices ($250). However, the liability on families/students can be reduced significantly by checking with your local insurance agent.

My child forgot to charge their Chromebook before school. Now what?
Students are expected to charge their Chromebooks nightly at home and bring them to school fully charged. If one is available, students who do not bring a charged Chromebook back to school may be issued a loaner device (DELL computer) for the day, which cannot be taken home. The loaners will be in the library for students to check out if available. Loaners may not be available and your student may be without the Chromebook for the day. They may be able to charge the Chromebook in the library during breaks or lunch. If this happens often, then discipline action may be taken.

How will students carry their Chromebook from class to class?
Chromebooks should never be transported while open as even gentle handling can damage the screen. Chromebooks should be safely closed and placed in a backpack before they are taken from classroom to classroom, or to and from school. The backpacks provided will have space for the device's charger.

Return
Students will return their fully functional device at the end of each school year. All of the following must be returned: Chromebook, charger, and chromebook backpack. Upon transfer or termination, any device not returned within 5 days will be reported as stolen and a police report will be filed.

Care and Maintenance
Devices must remain **free** of any stickers, drawings, writings, or labels that are not the property of Dyersburg City Schools.
Only a clean, soft cloth should be used to clean the laptop screen; cleaners of any type should **not** be used. If the screen needs more cleaning than a dry cloth can offer, students should bring the device to the library.
Special caution should be used to **not** place excessive pressure or weight on the device.

1:1 CHROMEBOOK FAQS

How is one student's Chromebook identified from another student?
All the Chromebooks are the same, so they look very much alike. However, each Chromebook will be tagged with a sticker with a number that is assigned to this particular student. Additionally, each device has a serial and model number. The district keeps all that data, so if a Chromebook is misplaced, we can determine who it is assigned to get it back to the student user. Any ID stickers that are on the Chromebook when issued must stay on the Chromebook. No additional permanent markings of any kind (stickers, engraving, permanent ink pen, tape, etc.) shall be placed on the Chromebook or it's backpack at any time. While the devices are issued to students, they are still school-owned property. Additional permanent markings on the device or its backpack will be considered vandalism. Students can add non-permanent identifying items to the case such as ribbon, key chains or other removable items. Each student will also receive a charger. The charger will also have the same number on it as the Chromebook. **DMS students will not take chromebooks home at this time.**

Will the Chromebooks ever leave the building?
DMS students will not take chromebooks home at this time.
Students will be allowed to take the Chromebooks home for school-related use. All students must have a Chromebook Technology User Consent Form and a Student Equipment Agreement Form signed by themselves and a parent before they are issued a Chromebook.

What happens if the device is damaged or lost?
Students and parents will be responsible for school-owned technology property that is issued to them, just as they are for other school-owned items such as textbooks, calculators, cameras, athletics equipment or library books. The district will repair or replace the device, but students and parents will be responsible for the cost of those repairs or replaced devices ($250). However, the liability on families/students can be reduced significantly by checking with your local insurance agent.

My child forgot to charge their Chromebook before school. Now what?
DMS students will not take chromebooks home at this time.
Students are expected to charge their Chromebooks nightly at home and bring them to school fully charged. If one is available, students who do not bring a charged Chromebook back to school may be issued a loaner device (DELL computer) for the day, which cannot be taken home. The loaners will be in the library for students to check out if available. Loaners may not be available and your student may be without the Chromebook for the day. They may be able to charge the Chromebook in the library during breaks or lunch. If this happens often, then discipline action may be taken.

How will students carry their Chromebook from class to class?
Chromebooks should never be transported while open as even gentle handling can damage the screen. Chromebooks should be safely closed and placed in a backpack before they are taken from classroom to classroom, or to and from school. The backpacks provided will have space for the device's charger.

Where can you get an Internet connection if the building's wireless connection is not working?
The devices will only connect to the web wirelessly. If the district's WiFi network is down during school, the Chromebooks will not have connectivity to the web. However, some features, such as access to the student's Google Drive, will still work on a limited basis. The work that is done off-line will not be backed up until a wireless Internet connection is restored. The public library in Dyersburg has public WiFi access.

What login will students use to get into the device operating system?
Students will each have an Email address that is their primary login and username. Students can change their password, but they cannot change their username. The district can reset a password, however, the student should do their best to remember passwords to ensure successful logins.

Can the Chromebooks be used with another username?
No. Students and staff cannot access a district-owned Chromebook with any other login other than their district-assigned Email. For example, students will not be able log in to their personal Gmail account on a district-provided Chromebook. However, if a student logs into another device with their school username (a PC laptop, a school lab computer, a loaner Chromebook, etc.) all of their information (bookmarks, Emails, documents, applications, etc.) will be available to them on that device when using a Chrome browser.

Will unsafe or inappropriate websites be filtered on the devices?
We do our best to ensure your child's online experience is safe. Before each Chromebook device connects to the Internet, it must pass through district network firewalls and filters. This happens whether the device is browsing on campus on school-owned networks, or off campus using another WiFi router that is providing the Internet connection. If your child is using the Chromebook at school, at home or at a public library, it will always pass through our web filtering system before they can see or access web content. Our web filters are programmed to block inappropriate content as much as possible.

What happens if students have been visiting inappropriate websites?
While we do our best to stay on top of things, some websites are not blocked or are able to bypass our filters. Teachers and parents are encouraged to randomly check the browsing history of student Chromebooks on a regular basis. Browsing histories cannot be deleted by the students. The district will also conduct random checks of student browsing histories. If you discover any inappropriate web activity, please contact your child's teacher, building principal or assistant principal. Inappropriate web browsing is a violation of the district Internet Acceptable Use Policy and may result in disciplinary action.

What if another student damages my student's device?
In such cases, circumstances will be investigated on a case-by-case basis. School administration and the School Resource Officer may be involved if it is suspected to be an intentional act or act of vandalism.

Can you print from the devices?
Digital online file sharing between staff and students is one of the great advantages of the Chromebooks and is an easy and efficient way to distribute and turn in assignments without printing. It also saves on paper, ink and toner use, thereby saving the district money. Students can print to several new printers in the building.

Who is responsible for updating the device (software and applications)?
The Chromebook operating system, Chrome OS, updates itself automatically. Students do not need to manually update their Chromebooks. Chromebooks use the principle of “defense in depth” to provide multiple layers of protection against viruses and malware, including data encryption and verified boot. By logging in with their school Email account Chromebooks seamlessly integrate with the Google Apps for Education suite of productivity and collaboration tools. This suite includes Google Docs (word processing), Spreadsheets, Presentations, Drawings, and Forms.

Can students download apps?
No. Student access to the web store is limited.

How can students submit work or assignments via their devices?
Google Drive/Classroom has features built into it that allow work to be “shared” between teachers and even classmates. Students can create documents, spreadsheets, drawings, photos, presentations and even videos. Each item can be “shared” with a teacher prior to its due date. The teacher can then see the work on his or her own computer to review it or grade it for the student.

Can the devices be used at home?
Yes, if your home has a WiFi network, the devices will have the same filtered web access as they would at school. If you don’t have a WiFi network at home, students can still use them, but in a limited capacity. Some applications will work “offline” (such as Google drive) but content saved to the device will not be backed up online until Internet connection is available for the device.

Will devices be kept by students over summer?
No. Devices will be turned in at the end of the school year so the district can do maintenance on them. Devices will be re-issued at the start of the school year to continuing students. Devices issued to students who leave the district (move, etc.) will be reformatted and re-issued to other students on an as-needed basis. **DMS students will not take chromebooks home at this time.**

Can the school track web history?
Yes. The school can track information on what sites students were on, when they were on them, and how long they were on those sites. Students should only visit sites that are approved by the district and those that are not in violation of the Responsible Use Policy. Violations of the policy can result in disciplinary action, including the student being suspended from using the school network and device use.

How can you prevent student copying and/or plagiarism?
There are ways within the software systems we have to check and see if work is copied between students. We are also looking at software to help prevent cheating from happening.

Can parents use the Chromebooks?
When a student is logged into the Chromebook, parents can use them to check on student work, view their browsing history or connect with teachers through our Synergy parent portal or via the student's Email. The Chromebooks are not intended for personal use for the student or their parents.

Can student work be transferred from their Chromebook to another device?
Student applications, Emails, bookmarks, documents, presentations and just about anything done in the Chrome browser while a student is logged in is available on another Chrome browser on another device when the student logs in with his or her district Email address. The content will be the same on the Chromebook as it is, say, on a PC desktop computer, so long as students are using a Chrome browser and their Email login. Data can also be saved to a USB drive and transported between devices.

Distribution/ Return Plan

Distribution Process
At the beginning of each school year, each student will be given a DCS Chromebook Responsible Use Policy and it will have to go home and be signed by the student and parent. Once these papers are returned signed, the student will be assigned a Chromebook.

Return
DMS students will not take chromebooks home at this time unless they are EXT.
Students will return their fully functional device at the end of each school year. All of the following must be returned: Chromebook, charger, and chromebook backpack. Upon transfer or termination, any device not returned within 5 days will be reported as stolen and a police report will be filed.
Devices go through standard maintenance and re-imaging over the summer, but the same device is reissued to the same student the following school year. The device and accessories remain the property of Dyersburg Middle School. The high school reserves the right to collect and/or inspect a student's device at any time and to delete any material or applications deemed inappropriate. Sleeves insured by the district to protect devices follow the device through the four-year cycle. Use of a device sleeve and backpack is required. Replacement for any reason will be at the user's expense.
Report cards or diplomas can be held from students who do not return devices at the end of the school year. Continued failure to return a device will result in the district filing a theft report. The student will be responsible for intentional damage to the laptop and accessories – in which case payment for repair or replacement will be required.

Student Use of Technology

Charging the battery: **DMS students will not take chromebooks home at this time.** Students must arrive each day with a fully charged device and a charger. As is the case with many electronic devices, including cellular phones, computer devices generally need to be plugged into an electrical outlet for several hours to fully charge. Students should not expect to charge devices at school. Being prepared for class includes having a fully charged device.

Probationary Student Privileges: DMS students will not take chromebooks home at this time. To protect the assets of the DCS, some students will be required to turn in their Chromebooks to the school library at the end of each day for a period to be determined unless otherwise specified in the Responsible Use Policy. The librarian will secure the equipment during the evening and the student will be allowed to check it back out on a daily basis.

Students who will be included as probationary will be the following:

Students who have violated any Use Policy during the current or previous semester.

Chromebooks left at home: DMS students will not take chromebooks home at this time. If students leave their Chromebook at home, they will be allowed to phone their parent/guardian to bring it to school prior to 8:00 A.M. If unable to contact parents, the student will have the opportunity to use a replacement device from the library if one is available. Repeat violations of this policy will result in disciplinary action.

Sound: Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes. Headphones may be used at the discretion of the teacher.

Equipment: As with any school property, students are fiscally responsible for damage to devices. Student devices will be periodically checked for physical condition and acceptable use. Students leaving the district must return district equipment by the last day of attendance. Each device has an asset tag and certificate of authenticity (COA) that should never be removed for any reason.

Accidental Damage/Loss: The 1:1 User's Charge will cover most damages that are deemed accidental. Loss or damage due to negligence will be the responsibility of the parent/guardian. When damage occurs, a replacement machine will be issued until all repairs are complete. Parents/guardians are not authorized to attempt repair or secure the services of a technician for repairs – as this may void the manufacturer's warranty.

Code of Conduct: The school will create and administer behavior plans and consequences related to proper use of technology. All students will follow the content of the Responsible Use Policy and the 1:1 Website. School handbooks and student discipline codes will direct actions within the school. Accidental damage, loss, or theft are the responsibility of the parent/guardian and covered elsewhere in this resource guide. The process for reporting damage starts at the school level, where personnel will investigate damages and make a determination of misuse or accidental damage. The school Tech Team will handle accidental damage. A loaner machine will be provided until the school-issued device can be repaired and returned to the student. All

offenses of misuse or abuse of the device will be elevated to a school administrator. The school will follow a hierarchy of consequences based on aggravating and mitigating discipline factors. Potential consequences could include, but are not limited to, verbal warnings, seating assignments, after school detention, suspension of technology use, limited to day-use only, or revoking all device privileges.

TIPS for Device Use at HOME-DMS students will not take chromebooks home at this time.
-- Charge your device at home daily
-- Set guidelines as a family for where and when the device can be used at home
-- Ask questions when the site history on a computer is cleared
-- Get parental permission before sharing photos or videos of others
-- Abide by the 1:1 Guidelines and Responsible Use Policy
-- Discuss safe online practices as a family
-- Use necessary precautions to protect electronic devices from damage

Device User's Guide

A. Care and Maintenance

General precautions: Devices must remain free of any stickers, drawings, writings, or labels that are not the property of the Dyersburg Middle School.

Only a clean, soft cloth should be used to clean the laptop screen; cleaners of any type should not be used. If the screen needs more cleaning than a dry cloth can offer, students should bring the device to the library.

Special caution should be used to not place excessive pressure or weight on the device.

Avoid eating or drinking while using the device and do not expose the device to extreme temperatures. Be cautious when using the device in an area where pets may damage the unit.

Be very careful to avoid bumping the device against corners, walls, lockers, floors, etc.

Carrying a device: Devices should be carried in a backpack.

Storage: DMS students will not take chromebooks home at this time.
Each student is encouraged to take his/her device home each day. When not in use, devices should be stored in a safe and secure place. Do not leave devices in an unlocked locker or automobile.

Lost or stolen device: DMS students will not take chromebooks home at this time.
Families are responsible for returning the device in working order. Charges apply for any unit returned with damages or not returned at all. Third-party insurance is available against theft, burglary, or robbery during deployment. Families without this or other insurance will be billed for the full cost of replacement or repair ($250).

Battery: Students are responsible for keeping the chromebook battery charged for school each day by returning it to the assigned cart at the end of each day.

File Management: Students must follow all advice given by teachers and technology coordinators at their school. Generally, all student data must be backed-up daily.

Pre-installed Software: Students are not allowed to load any new software, uninstall software, or add other applications without the approval of the school technology coordinator.

Personalization: Students should follow school-specific guidelines for personalization of school issued backpack or the device itself. Do not add any stickers or other identifying marks, without checking with the school first. Never change the device settings, without approval from the school technology coordinator.

B. Technical Support

Repair: Parents, guardians, or students are **not** allowed to attempt repairs themselves or contract with any other individual or business to repair school owned equipment. All repairs will be performed by Dyersburg City Schools. Self-repair will void any manufacturer warranties and protection plans. Services offered by Tech Support personnel include login assistance, loaning devices, technical or software problem resolution, reporting website concerns, reporting devices as lost, stolen, or damaged, and more.

Replacement: Students with a school issued device needing repair or replacement will receive a loaner device. This process will be managed by the technology coordinator at each school. All responsibilities and guidelines for use will apply to the replacement device as well.

Damage Fees: Each incident of damage will be reviewed by the technology department and prices for damages and repair will be handled on an individual basis with the parent/guardian. All repairs must be made by school district staff and not a third party technician. Some repairs may be covered under the device warranty, but anything outside that cost will be covered by the parent/guardian.

C. Printing: The requirement to print will be limited for most students, but when needed, students can save files to cloud or external storage and print via devices at-home or other locations. No external printer drivers can be loaded on district devices.

D. Device Security and Safety: School-issued devices are configured so that the student can login under his/her assigned network username and password.

In accordance with the Children's Internet Protection Act (CIPA), all devices reside on the district's network. The district maintains an Internet content filter. Filtering, however, is not as reliable as adult supervision. Student Internet use on district-issued devices will be filtered through the district's Internet content filter regardless of home or school use. There should be no expectation of privacy when using devices and curriculum resources. When students are either on campus or at home using school-provided devices, the filter kicks content back to our server.

As needed, the filter can be programmed to add or remove blocks or allow additional content for educational purposes. Any attempts to bypass the filter or visit unacceptable sites constitute a violation of the Responsibility agreement. While it is impossible to predict with certainty what information on the internet students may access or obtain, school district personnel shall take every reasonable precaution to prevent students from accessing material and information that is obscene, pornographic, or otherwise harmful to minors, including violence, nudity, or graphic language that does not serve a legitimate pedagogical purpose. These procedures comply with board policy and the mandates of CIPA. DMS is not responsible for the content accessed by users who connect to the internet via their personal mobile technology.

When using school or district provided software or programs, special permission is required to post pictures or video that includes images of students. School district personnel follow strict guidelines to protect student privacy and all students and families should seek approval from school personnel to post video or pictures that include students. Parents should consider terms and conditions of use, as well as any legal responsibilities, before allowing photos, audio, or video of minors to be posted online when using any software or programs. We take student privacy seriously and so should you! In accordance with district policy, cyberbullying is unacceptable and will not be tolerated. Students must not share their login information and passwords with other students, and students should not loan out a device or log in as someone else.

E. Parental Consent: The board recognizes that parents of minors are responsible for setting and conveying the standards their children should follow when using media and information sources. Accordingly, before a student may independently access the Internet, the student's parents must be made aware of the possibility that the student could obtain access to inappropriate material while engaged in independent use of the Internet. The parent and student must consent to the student's independent access to the Internet and to monitor the student's Email by school personnel.

In addition, in accordance with the board's goals and visions for technology, students may require accounts in third party systems for school related projects designed to assist students in mastering effective and proper online communications or to meet other education goals. Parental permissions will be obtained when necessary to create and manage such necessary third party accounts.

F. Privacy: No right of privacy exists in the use of technological resources. Users should not assume that files or communications accessed, downloaded, created, or transmitted using school district technological resources or stored on services or hard drives of individual computers will be private. School administrators or individuals designated by the Director of Schools may review files, monitor all communication, and intercept Email messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School district personnel shall monitor on-line activities of individuals who access the Internet via a school owned device.

Under certain circumstances, the board may be required to disclose such electronic information to law enforcement or other third parties, for example a response to a document production

request in a lawsuit against the board, as a response to public records requests or as evidence of illegal activity in a criminal investigation.

G. Social Media and Personal Websites: DCS may use any means available to request the removal of information on personal websites or social media sites that substantially disrupt the school environment. No one may utilize school district or individual school names, logos, or trademarks or unapproved pictures or recordings without permission. DMS recognizes and communicates that it is unlawful to publicly post or share pictures or media of other individuals without the consent of parents for minors.

Students: Though school personnel generally do not monitor students' Internet activity conducted on non-school district devices during non-school hours, when the student's online behavior has a direct and immediate effect on school safety or maintaining order and discipline in the schools, the students may be disciplined in accordance with board and school policy.

Replacement costs for the Chromebooks are as follows:

- Chromebook: $250.00
- Power Supply: $35.00 (not applicable to DMS)
- Chromebook backpack: $15.00

Responsible Use Policy (RUP)

Internet access* is available for all students only as an educational resource.

- I will not go to websites that are not appropriate for learning.
- I will inform a teacher immediately if any inappropriate sites are accessed while I am online.
- I will not attempt to bypass the Internet filter to access a blocked website.
- I will not remotely access computers outside the system's network. *Internet access is provided on-campus for all students. These policies also apply when using school-issued devices off-campus through other public or private networks. The computer, software, wireless devices, and network are available for all students only as an educational resource.
- I will treat the computers, all devices, and hardware with respect and not cause damage to them.
- I will not share my usernames and passwords with anyone nor will I use another student's username and password.
- I will not share my device, charger, or other school-issued equipment with others.
- I will transport my device using my school-issued backpack and handle my device using communicated procedures.
- I will not access, alter, or delete another person's information/files on any computer or device.
- I will follow copyright law in my projects and give credit to my resources (authors and/or websites).
- I understand that teachers and administrators may monitor all student activities on the network and devices on and off campus.

● I will not use the device to illegally distribute, install, or reproduce copyrighted materials.
● I will not use the device to facilitate any illegal activity or use it for commercial or for-profit use.
● I will not use the computer network to attempt to gain unauthorized or unlawful access to other computers, computer systems, or accounts.
● I will not utilize my school name, logo, or trademark without permission.
● I understand that students are responsible for storing and backing up their own data.

School-issued devices are set-up and the software programs are selected for all students only as an education resource.

● I will not download, install, or remove software/apps or media without permission and direction from a teacher.
● I will not personalize the external appearance of my school-issued device.
● I will not change the school settings on my device.
● I will immediately notify my teacher or the building level technology coordinator if I identify a security problem or other issue on a technological resource, and I will not demonstrate the problem to others.

Good Digital Citizenship should be practiced on and off campus.

● I will only use online communication (Email, instant messaging, blogs, wikis, etc.) for educational purposes on school-issued devices.
● I understand that all school-issued Email communications are stored and may be accessed and examined by teachers and administrators at any time.
● I will always use proper and appropriate language and my best writing skills (including adhering to copyright policies).
● I will never give or post personal information (my name, address, telephone number, etc.) to someone online.
● I will never use online communication to harass or bully anyone.
● I will not engage in creating, intentionally viewing, accessing, downloading, storing, printing, or transmitting content that is obscene, profane, pornographic, harassing, abusive, or considered harmful to minors.
● I understand that I should not share or post pictures or recordings of other individuals without their consent (or parental consent for minors).

School Email

● Dyersburg City Schools may provide students with a closed-campus Email account.
● Email usage may be monitored and archived. There is no expectation of privacy with school Email accounts.

I**f I don't follow the RUP:**

● I may lose the privilege of using computers, personal devices, and/or the Internet at school.
● I may lose the privilege of taking a device off-campus.
● I understand that I may be held financially responsible for any deliberate or negligent damage to equipment and for loss or theft of the equipment while in my possession or when I am charged with its care (see below).
● I understand that the administration will determine disciplinary and/or financial consequences for Responsible Use Policy (RUP) violations.

● I understand that certain willful misuse may result in criminal prosecution under applicable state and federal law.

Authorized Use Policy

A. Introduction

It is the policy of the school to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106554 and 47 USC 254(h)].

B. Access to Inappropriate Material

To the extent practical, technology protection measures shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

C. Internet Safety

Training In compliance with the Children's Internet Protection Act, each year, all DMS students will receive internet safety training which will educate students about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyberbullying awareness and response. Such training will include Internet, cell phones, text messages, chat rooms, Email and instant messaging programs.

D. Inappropriate Network Usage

To the extent practical, steps shall be taken to promote the safety and security of users of the District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

E . Supervision and Monitoring

It shall be the responsibility of all school employees to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act.

Internet Usage Personal Responsibility

One fundamental need for acceptable student use of school electronic resources is respect for, and protection of, password/account code security, as well as restricted databases files, and information banks. Personal passwords/account codes may be created to protect students utilizing electronic resources to conduct research or complete work.

These passwords/account codes shall not be shared with others; nor shall students use another party's password except in the authorized maintenance and monitoring of the network. The maintenance of strict control of passwords/account codes protects employees and students from wrongful accusation of misuse of electronic resources or violation of school policy, state or federal law. Students or employees who misuse electronic resources or who violate laws will be disciplined at a level appropriate to the seriousness of the misuse.

Acceptable Use

The use of the DMS technology and electronic resources is a privilege, which may be revoked at any time. Students are only allowed to conduct electronic network based activities which are classroom or workplace related. Behaviors which shall result in revocation of access shall include, but will not be limited to: damage

to or theft of system hardware or software; alteration of system hardware or software; placement of unlawful information, computer viruses or harmful programs on, or through the computer system; entry into restricted information on systems or network files in violation of password/account code restrictions; violation of other users' rights to privacy; unauthorized disclosure, use or dissemination of personal information regarding minors; using another person's name/password/account to send or receive messages on the network; sending or receiving personal messages on the network; and use of the network for personal gain, commercial purposes, or to engage in political activity.

Students may not claim personal copyright privileges over files, data or materials developed in the scope of their school, nor may students use copyrighted materials without the permission of the copyright holder. The Internet allows access to a wide variety of media. Even though it is possible to download most of these materials, students shall not create or maintain archival copies of these materials unless the source indicates that the materials are in the public domain.

Access to electronic mail (Email) is a privilege and designed to assist students in the acquisition of knowledge and in efficiently communicating with others. The District Email system is designed solely for educational and work related purposes. Email files are subject to review by District and school personnel . Chain letters, "chat rooms" or Multiple User Dimensions (MUDs) are not allowed, with the exception of those bulletin boards or "chat" groups that are created by teachers for specific instructional purposes or employees for specific work related communication.

Students who engage in "hacking" are subject to loss of privileges and school discipline, as well as the enforcement of any District policy, state and/or federal laws that may have been violated. Hacking may be described as the unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems, or programs, or other property of the school, a business, or any other governmental agency obtained through unauthorized means.

To the maximum extent permitted by law, students are not permitted to obtain, download, view or otherwise gain access to "inappropriate matter" which includes materials that may be deemed inappropriate to minors, unlawful, abusive, obscene, pornographic, descriptive of destructive devices, or otherwise objectionable under current District policy or legal definitions.

The school administration reserves the right to remove files, limit or deny access, and refer students violating the Board policy to appropriate authorities or for other disciplinary action.

Privileges

The use of school technology and electronic resources is a privilege, not a right, and inappropriate use will result in the cancellation of those privileges. All students who receive a password/account code will participate in an orientation or training course regarding proper behavior and use of the network. The password/account code may be suspended or closed upon the finding of user misuse of the technology system or its resources.

Network Etiquette and Privacy

Students are expected to abide by the generally accepted rules of electronic network etiquette. These include, but are not limited to, the following:
1. System users are expected to be polite. They may not send abusive, insulting, harassing, or threatening messages to others.
2. System users are expected to use appropriate language; language that uses vulgarities or obscenities, libels others, or uses other inappropriate references is prohibited.

3. System users may not reveal their personal addresses, their telephone numbers or the addresses or telephone numbers of students, employees, or other individuals during Email transmissions.
4. System users may not use the District's electronic network in such a manner that would damage, disrupt, or prohibit the use of the network by other users.
5. System users should assume that all communications and information is public when transmitted via the network and may be viewed by other users. The school administrators may access and read Email on a random basis.
6. Use of the District's electronic network for unlawful purposes will not be tolerated and is prohibited.

Personal Technology Devices and the District's Wireless Internet Network

A "personal technology device" is defined as any privately owned electronic and/or wireless device, including but not limited to: laptop and mobile computers, tablet computers, mobile phones, smart phones, Personal Digital Assistants (PDAs), ebook readers, camcorders, cameras, audio players (iPods, MP3 players, etc.), handheld entertainment systems, and any device that can be used for office applications, word processing, Email communication, wireless Internet access, making or receiving text messages or telephone calls, information transmitting/receiving/storing, video recording, image capturing/recording, and/or sound recording.

The school permits students to bring their personal technology devices to school and to access the District's wireless Internet network under the following express conditions:
1. Before bringing any personal technology device(s) to school, students must sign the School's "Technology User Consent Form" and submit the signed Form to the school. If the school does not have a signed Form on file for a student, and the student is observed with a personal technology device, then the device will be confiscated from the student and will not be returned to the student until the end of the school day.
2. The school does not provide technical support for personal technology devices.
3. Students will access the District's wireless Internet network with the username and login provided to them and assigned to them by the District; students are not permitted to access the District's wireless Internet network as a guest or using a guest user name/login.
4. Use of personal technology devices on the District's wireless Internet network will be for educational purposes only.
5. The school is not responsible for the damage, loss, or theft of any personal technology device.
6. The school is not responsible for the security of any personal technology device including, but not limited to, virus protection and/or unauthorized release of information contained on the device. The school recommends that any personally sensitive files and information (such as tax documents, social security information, bank records, etc.) be removed from the personal technology device before it is brought to school or used at school.
7. Students will respect the privacy of other students when using personal technology devices, including those personal technology devices that have video recording, image capturing/recording, and/or sound recording capabilities. Students will not take or share video recordings, images, or sound recordings at school or in connection with a class or school activity without express permission from a teacher or administrator.
8. When using any personal technology devices, students must comply with all Board of Education policies and regulations, including, but not limited to, this Regulation regarding acceptable use of District technology and electronic resources and all federal, state, and local laws.
9. When using personal technology devices, staff must comply with Board of Education Policy 4650 regarding communication with students by electronic media.
10. Personal technology devices must be configured to minimize the ability of unauthorized individuals to monitor data communications or to gain access to the District's wireless Internet network, wired network, or other District resources.

11. If any personal technology device or wireless access point disrupts services provided by the school, or behaves in such a way that the service or security of the school is degraded, the school reserves the right to permanently disconnect that device from the school's wireless Internet network.
12. Parents who choose to allow students to use their own personal technology devices and students who bring their own personal technology devices to campus do so knowing that it will diminish their expectation of privacy regarding their personal technology device while at school. The school reserves the right to search personal technology devices in accordance with applicable laws and policies if there is reasonable suspicion that the student has violated the school's policies, procedures or rules, or engaged in other misconduct while using the personal technology device. Violation of the school's policies or local, state and/or federal laws will result in revocation of the privileges given under this regulation.
13. The school has the right to collect and examine any personal technology device that is suspected of causing problems or was the source of an attack or virus infection on the school's wireless network.

By logging onto or accessing the school's wireless network, students are agreeing to the above listed conditions. In the event that a student uses the school's wireless network on a personal technology device in an inappropriate or unacceptable manner at any time OR uses a personal technology device using an outside service provider in an inappropriate or unacceptable manner during the school day, in violation of Board policies, or in violation of these guidelines, the student or staff member will be subject to disciplinary action.

Third Party Software Applications and Web-Based Services

The school utilizes computer software applications and web based services operated not by the school but by third parties. These include Google Apps for Education, and similar educational programs. In order for students to use these programs and services, certain personal information – generally the student's name and Email address – must be provided to the third party operator.

Technology use in the school is governed by federal laws and regulations including:
Children's Online Privacy Protection Act (COPPA)
COPPA applies to commercial companies and limits their ability to collect personal information from children under 13. These programs must provide parental notification and obtain parental consent before collecting personal information from children under the age of 13. The law permits the school to consent to the collection of personal information on behalf of all of its students, thereby eliminating the need for individual parental consent given directly to the third party operator. The Technology User Consent Form allows the school to act as an agent for parents in the collection of personal information within the school context. The Technology User Consent Form constitutes consent for your student and/or the school to provide personal information to third party operators. No personal student information is collected for commercial purposes. The school's use of student personal information is solely for education purposes. For more information on COPPA, please visit:
https://www.ftc.gov/tipsadvice/businesscenter/guidance/complyingcoppafrequentlyaskedquestions.

Family Educational Rights and Privacy Act (FERPA)
FERPA protects the privacy of student education records from unauthorized disclosure. FERPA gives parents the right to access their children's education records and the right to consent to disclosure of personally identifiable information from the records.Under FERPA, schools may disclose directory information (see Board Policy and Regulation 2400). The term "education records" is defined as those records that contain information directly related to a student and which are maintained by an educational agency. FERPA allows "school officials" to obtain access to personally identifiable information contained in education records provided the school has determined that the official has a "legitimate educational interest" in the information. All students who return the Technology User Consent Form will be assigned an Email account through Google Apps for Education. This account will be considered the student's official school Email address until such time as the student is no longer enrolled with the school.

Services

While the school is providing access to electronic resources, it makes no warranties, whether expressed or implied, for these services. The school may not be held responsible for any damages including loss of data as a result of delays, non-delivery or service interruptions caused by the information system or the user's errors or omissions. The use or distribution of any information that is obtained through the information system is at the user's own risk. The school specifically denies any responsibility for the accuracy of information obtained through Internet services.

Security

The Board recognizes that security on the school's electronic network is an extremely high priority. Security poses challenges for collective and individual users. Any intrusion into secure areas by those not permitted such privileges creates a risk for all users of the information system.

The account codes/passwords provided to each user are intended for the exclusive use of that person. Any problems, which arise from the user sharing his/her account code/password, are the responsibility of the account holder. Any misuse may result in the suspension or revocation of account privileges. The use of an account by someone other than the registered holder will be grounds for loss of access privileges to the information system.

Users are required to report immediately any abnormality in the system as soon as they observe it. Abnormalities should be reported to the classroom teacher or system administrator.

The school shall use filtering, blocking or other technology to protect students and staff from accessing internet sites that contain visual depictions that are obscene, pornographic or harmful to minors. Do not attempt to override the Internet filtering software or other network configurations . The school shall comply with the applicable provisions of the Children's Internet Protection Act (CIPA), and the Neighborhood Internet Protection Act (NCIPA).

Vandalism of the Electronic Network or Technology System

Vandalism is defined as any malicious attempt to alter, harm, or destroy equipment or data of another user, the school information service, or the other networks that are connected to the Internet. This includes, but is not limited to the uploading or the creation of computer viruses, the alteration of data, or the theft of restricted information. Any vandalism of the school electronic network or technology system will result in the immediate loss of computer service, disciplinary action and, if appropriate, referral to law enforcement officials.

Student Email Agreement

My signature below signifies my understanding that DMS Schools Email accounts are for educational purposes only and provided as a privilege by DMS. Any misuse of the DMS Email system will result in immediate cancellation of my account. Malicious and/or illegal misuse of my Email account, computer files or system network could result in legal prosecution. My signature below also signifies that I will not share my password with anyone.

As a student of DMS, I hereby state that I have read and understand the Use of Internet and Internet Safety Policy as printed on the back of this form, and that I agree to comply with the provisions stated therein.

I further state that I understand the following:
1. Teachers, network and/or site administrators may review any files and communications to maintain system integrity and ensure that students are using the system responsibly. All student Email is archived in accordance with Federal regulation.

2. Files and any other information or communication stored on any electronic equipment owned or operated by Dyersburg City Schools are not private and will not be maintained indefinitely.
3. Failure to abide by the terms of this agreement may result in disciplinary action up to criminal prosecution by government authorities.

Consequences

The consequences for violating the School's Acceptable Use Policy include, but are not limited to, one or more of the following:
1. Suspension of District Network privileges;
2. Revocation of Network privileges;
3. Suspension of Internet access;
4. Revocation of Internet access;
5. Suspension of computer access;
6. Revocation of computer access;
7. School suspension;
8. Expulsion;

Authorized Usage
TECHNOLOGY USER CONSENT FORM

Student Consent

I have read and understand the Dyersburg Middle School Authorized Usage Policy and agree to abide by them. I understand that violation of the Policy and/or Regulation may result in disciplinary action taken against me and could also include suspension or expulsion from school.
I understand that my use of the district's technology is not private and that the school district may monitor my use of district technology, including but not limited to accessing browser logs, Email logs, and any other history of use. I consent to district interception of or access to all communication I send, receive, and store using the district's technology resources, pursuant to state and federal law, even if the district's technology resources are accessed remotely.
I understand that bringing my own personal technology devices to campus will diminish my expectation of privacy regarding my personal technology devices while at school, and that the District reserves the right to search my personal technology devices in accordance with applicable laws and policies if there is reasonable suspicion that I have violated the District's policies, procedures or rules, or engaged in other misconduct while using my personal technology devices.

Signature of Student Grade Student ID Date

Printed Signature of Student

Parent/Guardian Consent

I have read and understand Dyersburg Middle School Authorized Usage Policy. I hereby give permission for my student to utilize the District's technology resources, including Google Apps for Education, and use his or her own personal technology devices while at school.
In consideration for my student being able to use the District's technology, use the District's network or internet, and/or bring their own personal technology devices to school, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my student's use of, or inability to use, the District's network or technology, or and my student's use of his or her own personal technology device.
I hereby authorize the District to act as an agent for me in the collection of information within the school context while my student is using the District's technology resources or his or her own personal technology devices.
I understand that my student's use of the district's technology is not private and that the school district may monitor his or her use of district technology, including but not limited to accessing browser logs, Email logs, and any other history of use. I consent to district interception of or access to all communication my student sends, receives, and stores using the district's technology resources, pursuant to state and federal law, even if the district's technology resources are accessed remotely.
I understand that my student bringing his or her own personal technology devices to campus will diminish my student's expectation of privacy regarding his or her personal technology devices while at school, and that the District reserves the right to search my student's personal technology devices in accordance with applicable laws and policies if there is reasonable suspicion that my student has violated the District's policies, procedures or rules, or engaged in other misconduct while using his or her personal technology devices.
I agree to be responsible for any unauthorized costs arising from use of the District's technology resources by my student. I further agree to be responsible for any damages incurred by my student in using the District's technology resources or my student's personal technology device.

Signature of Parent/Guardian Date

Printed Signature of Parent/Guardian

Student Equipment Agreement Form

Student ID: _____ **School Year: __21-22_____**

Last Name: _____ **First Name: _____**

DMS Tag Number: _____ **Serial #:_____**

BORROWER'S AGREEMENT: The borrower (student/parent named below) agrees to assume full responsibility for the safety, care and maintenance of the chromebook. While the chromebook is in the borrower's possession, the borrower agrees to abide by all DMS Policies.

The chromebook is the property of the school district, and as such, is subject to monitoring and search of contents at any time. Please note that there is NO expectation of privacy in location, use or data stored on the chromebook. The device must be returned to the district immediately upon request, at the end of the year, or upon departure or termination from the District.

Replacement costs for the Chromebooks are as follows:

- Chromebook: $250.00
- Power Supply: $35.00 (not applicable to DMS)
- Chromebook backpack: $15.00

While the equipment is in my possession, I agree to the following:

1. I will take care of my chromebook as identified in the DMS Chromebook Procedures.
2. I will never leave the chromebook unattended and understand that if found at school, I will be subject to discipline. If my chromebook is damaged, lost or stolen I will report it to the school immediately.
3. I understand the chromebook is my responsibility and will not loan it to other individuals.
4. I will know where the chromebook is at all times.
5. I will bring a charged chromebook to school daily and will protect it by carrying it in the protective sleeve.
6. I will keep food and beverages away from my chromebook since they may cause damage to the device.
7. I will not disassemble any part of my chromebook or attempt any repairs.
8. I will use my chromebook in a way that is responsible and appropriate, meet DCS expectations and are educational.
9. I will not place decorations(such as labels,stickers,markers, etc.) on the chromebook. I will not deface the DCS identifiers on my chromebook.
10. I understand my chromebook is subject to inspection at any time, without notice and remains the property of the DCS. I will provide the chromebook passwords to staff immediately upon request.
11. I will follow the policies outlined in the chromebook Procedures while at school , as well as outside the school day.
12. I understand I am subject to disciplinary action if inappropriate content is found on the device. 13. I agree to return the DCS chromebook, power cords and any other accessories in good working condition.

Signatures below indicate I agree to the stipulations above and as outlined in the Chromebook Use, Policy, Procedures, and Information Guide. Copies of the chromebook handbook are available in the front office

Student Signature:_____

Grade: _____ **Date: _____**

Parent/Guardian Signature: _____

Address: _____

City: _____ State: _____Zip Code: _____ Email: _____

Home Phone: _____ Cell: _____ Work: _____