



Dyer County Schools 1:1 Chromebook Responsible Use Policy, Procedures and Information Guide

DCS Chromebook Assigned to Me

Name: _____

Model #: _____

DCS Asset #: _____

Serial #: _____

Dyer County Schools 1:1 Laptop Program

Dyer County Schools is committed to providing innovative ways for students to learn and is working hard to improve the quality and access to technology tools and resources. Essential to this effort is not just a computer device but a partnership between the District Curriculum Department and the schools that includes a willingness of the teachers to rethink the way they teach.

The policies, procedures and information within this document apply to all devices used in Dyer County Schools. Teachers may add requirements in their classrooms as they see fit.

Table of Contents

Chromebook FAQs 4

Distribution/Return Plans 8

Student Use of Technology 10

Device User's Guide 12

Responsible Use Policy 17

1:1 Responsibilities/Policies 19

Digital Citizenship 23

Student/Parent Responsibilities 26

District Copyright Guidance 28

1:1 Resources 32

Optional Insurance / Repair Costs 34

FORMS

Authorized Usage Policy 35

Technology User Consent Form 41

Student Email Account Agreement 42

Student Equipment Agreement Form 43

RUP AND WEB APPLICATIONS GUIDE 44

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 the student's name and student ID number on it. Additionally, district asset tags with barcodes will be on each device and each device has a serial 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 its carrying case at any time. While the devices are issued to students, they are still district-owned property. Additional permanent markings on the device or its case will be considered vandalism. Students can add non-permanent identifying items to the case such as ribbon, key chains or other removable items. Each carrying case will also have an ID tag attached to it, which should also stay on the exterior of the bag at all times.

Will the Chromebooks ever leave the building? Students grades 6-12 will be allowed to take the Chromebooks home for school-related use. All students must have a Chromebook Policy, Internet Acceptable Use Policy, and Media Release signed by themselves and a parent before they are issued a Chromebook. Students must also take the Responsibility Assurance Assessment prior to receiving a Chromebook.

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 for the day, which cannot be taken home. 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 a student must take it to another room, how will they carry their Chromebook?

Chromebooks should never be transported while open as even gentle handling can damage the screen. Chromebooks should be safely closed and placed in their travel case before they are taken from classroom to classroom, or to and from school. The cases provided will have a carrying strap and space for 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 Wi-Fi 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 Wi-Fi access. We are working on a growing list of business partners that will offer free Wi-Fi to DCHS students.

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 cannot recover passwords and students should remember them 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 Wi-Fi 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 happens if the device is damaged or lost? Students and parents will be responsible for district-owned technology property that is issued to them, just as they are for other district-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. However, the liability on families/students can be reduced significantly by taking part in the Chromebook Insurance Program or checking with your local insurance agent.

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. Printing has been disabled on the Chromebooks. Students will need to send anything they need printed to a teacher to have printed.

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.

How would you go about repairing a laptop that is not functioning? Damaged or non-functioning devices should be turned in to the student's library so a repair can be started. District technology staff members can repair many problems in-house, which may take a day or two. Other problems may require the devices being sent out for repair, which can take a several days or perhaps longer. Students who are without their device due to repairs will be issued a loaner to use during school only. Loaner devices must be returned to the library at the end of the school day.

Do repair fees need to be paid up front? Paying for repairs is preferred to be done up front, but in certain situations arrangements can be made for payment plans so students can continue using their device.

How much storage do students have? Students using Chromebooks will have 16 gigabytes (about 16,000 megabytes) of storage on the machine, plus an unlimited amount of online "cloud" storage that is attached to their Email and accessible via the Google Drive application.

What kind of APPLICATIONS are on the devices? There are thousands of apps available for Chromebooks covering a wide variety of topics. The apps, which run in the Chrome browser, are downloadable through the Chrome Web Store.

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.

What applications will be available on my child’s device? Different applications will appear on student devices depending on what grade the student is in or what classes they are enrolled in. The same goes for online textbooks.

What devices can be connected to a Chromebook? A Chromebook can connect to:

USB storage devices, mice and keyboards SIM cards SD cards External monitors and projectors (via HDMI)
Headphones, earbuds, microphones

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.

What if a student is out of school for an extended period (illness, travel, family emergency, etc.)? With the devices, it will become even easier for students to receive work from their teacher. Assignments, readings, and other resources can be placed online and shared with the student who is absent. The student can do the work online from home and share it back with the teacher.

Can the devices be used at home? Yes, if your home has a Wi-Fi network, the devices will have the same filtered web access as they would at school. If you don’t have a Wi-Fi 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 it an 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.

How long should Chromebooks last? Chromebooks have very few moving parts in them and generate very little heat. Therefore, the life expectancy — so long as they are treated appropriately — is fairly significant. Five years or more is not unrealistic. Additionally, the devices have powerful processors, adequate memory, and automatically update the latest software and security features without anything needing to be done by the student.

Can the district track web history? Yes. The district 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.

Are other districts doing this? Yes. We’ve been in contact with other districts around the state that have done one-to-one technology rollouts for students, including using Chromebook devices. There are also online resources about one-to-one programs in K-12 schools and we are using tips and advice from those sources, as well.

What can you say about eTextbooks? Will they replace traditional texts? There is a growing number of eTextbooks available for schools to use, whether they are viewed on Chromebooks, iPads, traditional laptops or other devices. e-texts are generally cheaper than hardcover textbooks, are updated at least annually (if not more often), are highly portable (multiple texts one device that weighs less than three pounds), and highly interactive. eTextbooks aren't just black letters on white screen. Often times, text is searchable, citable, linked to other resources, or chapters and lessons have learning activities, videos and photo galleries built right in. They are enhanced with audio, interactivity and multimedia, and they offer tremendous learning advantages to our students. We will still use traditional textbooks in the foreseeable future, but the shift to more eTextbooks will happen. Additionally, many of our curriculum pieces have online and interactive components to go along with the more traditional classroom materials.

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.

Will paper assignments become obsolete? We can't say we'll never have paper or printed projects or work, but it will become less used as time goes on. This can add up to significant cost savings for the district by using less ink, toner and paper. That's good for the environment, too.

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 my child opt out of having a Chromebook? No. Chromebooks are expected to become an integral part of the education all students receive at the Dyer County High School and we want them to take advantage of the powerful learning resources available with it.

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.

What about computer viruses getting onto the Chromebook? Since the applications run through the browser and online, there is little worry about having viruses infect the Chromebook's software or hardware.

What will it cost to charge the Chromebook at home? The electricity costs should be minimal to families over the school year, and the total cost is based on usage. Below is a formula to help you develop an estimate. The device draws about 40 watts, according to the manufacturer's specifications. To estimate electricity usage or kilowatt hours, use this formula: (Wattage x Hours plugged in per day x number of days per year) / 1000 = kWh Then multiply the answer by the average cost of electricity per kilowatt hour in Tennessee (about \$0.101). That is your estimate for the total annual cost. If your child uses or charges his/her Chromebook at home (they charge while being used, too) every day after school for two hours, the annual cost to parents is about \$1.45 (40 watts x 2 hour per day x 180 school days per year) / 1000 = 14.4 kWh 14.4 kWh x \$0.101 = \$1.45

1:1 Distribution/Return Plan

Distribution process

At the beginning of each school year, days are set aside for families (each enrolled student, with a parent or legal guardian) to attend a deployment session.

What you can expect at deployment:

Students must attend with a parent or legal guardian. In addition to a device, students will receive a power cord and protective sleeve during school day deployment. Parents and students will have an opportunity to learn more about the device and their responsibilities by viewing a presentation and reading the Responsible Use Policy (RUP). Staff will be available to answer any questions about the Resource Guide, RUP, or other policies.

Additional/optional 3rd party insurance will be available during deployment to cover theft, burglary, and robbery. All documents must be signed, payment made/arranged, and all steps in the process checked-off in order for the device to be released to the student during school day deployment.

Return

Students will return their fully functional device at the end of each school year in a process specific to each school. Both the device and power cord must be returned. 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 Dyer County Schools. The district 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 issued by the district to protect devices follow the device through the three-year cycle. Use of a device sleeve 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.

Home and School Use

Devices are purchased and equipped specifically for use at school and home. In addition to software, any device connected to the internet is filtered through the district purchased cloud server – offering additional protection against landing on an inappropriate or undesirable site. We are constantly working to improve the filtering integrity of our network, but rely on users (teachers, parents, and students) to guide these improvements. Parents and students are asked to report concerns about any site to the tech coordinator or administrator at their school. As always, adult supervision and parental guidelines are the best internet filtering available. District-issued devices are maintained by district personnel, and all devices are updated with the latest available software when available. Instructionally, teachers can easily give assignments for completion at-home or school when all students are using the same device and operational platform. Students without “at-home” privileges are required to arrive to school early enough to check-out a device for class before school begins. Likewise, students must take the time to return devices before departing for home each afternoon. Each school will establish detailed procedures for day-users.

Device Replacement

Students will be assigned a device and will use that same device, year-after-year, until the device is upgraded or replaced by the district. During the summer, devices will be collected and re-imaged, but reissued to the same student during deployment for the following school year. Should a device fail during the school year and require repairs, a loaner device may be issued to a student for the time it takes to repair the original device. As part of this process, it is important to remind students to regularly save all personal files to an external source or cloud storage. Some insurance companies offer coverage against theft – check with your insurance agent for details.

Wi-Fi Options

Accessibility to Wi-Fi is an important success factor for students at school and home. Our survey results from families indicate that a large majority of families have access to consistent and high-speed internet at-home. However, there are about 10-20% of our families who struggle with having reliable access to the internet at their residence. To serve these students in the early stages of 1:1, we are partnering throughout the community with business and industry, in the service and government sectors, and other groups and individuals to level the playing field by providing access close to the home or in the home of every student. Following is a summary of the options students have available to them for 1:1 educational work:

DCS Network @ School: All Dyer County schools are equipped with universal access to the internet for all students and staff. Work is ongoing to provide wireless access at the main entrance of each building – giving students additional after-hours access.

Student Use of Technology

Charging the battery: 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. **Backing-Up Files and Data:** Students supplied with a district-issued device are required to backup any files or data. It is the responsibility of each student to back up his or her own data. In the event a device is being serviced or swapped out with a loaner, it is critical to have access to all important files. **Probationary Student Privileges:** 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: 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 Chromebook 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.

BYOD – Bring Your Own Device: The instructional shifts and learning opportunities possible with 1:1 require that all students have access to the same information and tools as their classmates. Likewise, using the same device allows our technical team to address issues more expediently – preventing downtime that might interrupt student learning and class progress. Therefore, we are not allowing students to bring their own device to school (except for special circumstances approved by the classroom teachers or school administration). Dyer County Schools is not responsible for content viewed through personal devices or the damage, loss, or theft of personal devices. Code of Conduct: Each school site will create and administer behavior plans and consequences related to proper use of technology. All schools will follow the content of the Responsible Use Policy (RUP) and the 1:1 Website. School handbooks and student discipline codes will direct actions within each 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 Media Center 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. Each 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

-- 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 LCS 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 Dyer County School district.

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 help desk.

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 the district-provided protective sleeve. Schools may also require the sleeved-device to be carried in a student's backpack. Storage: 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: 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. Battery: Students are responsible for keeping the laptop battery charged for school 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 district-issued protective sleeves or the device itself. Do not add any stickers or other identifying marks, without checking with the school first. In an attempt to give students age-appropriate personalization options, this matter is not handled on a district level. 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 Dyer County 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 district-issued device needing repair or replacement will receive one from the district surplus inventory. 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

District-issued student 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 RUP 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. DCS 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 and Blackboard communication 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 district 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. DCS 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.

Employees' personal websites are subject to any and all regulations in the DCS Employee Code of Conduct.

A-Z QUICK TIPS for Device Users

- A. Keep the device secure and damage free.
- B. Protect the charger too – it is expensive to replace.
- C. Do not loan out the device, charger, or cords.
- D. Do not leave the device in any vehicle.
- E. Do not leave the device unattended.
- F. Do not have food or drinks in close proximity to the device.
- G. Do not allow pets near the device.
- H. Do not place the device on the floor or on a sitting area such as a chair or couch.
- I. Do not leave the device near table or desk edges.
- J. Do not stack objects on top of the device.
- K. Do not leave the device outside.
- L. Do not leave the device near pools or bathtubs.
- M. Do not check the device as luggage at the airport.
- N. Back up data and other important files regularly. DCS will at times perform maintenance on devices by imaging. All files not backed up to server storage space or other storage devices will be deleted during the process.
- O. Ensure devices are fully charged prior to arriving at school each day. P. Students should not deface, damage, or decorate their device in any way (i.e. marking, drawing, stickers, glitter, popping off keys).
- Q. Students are responsible for the care and cleaning of their laptop (cleaning screen and keyboard with a lightly damp cloth only and never using chemical cleaners on the laptop).
- R. Students should use care when plugging things into their laptop.
- S. The laptop should be completely closed when placed in a backpack.
- T. Do not place devices and power adapters under soft items (like blankets). Doing so can cause these items to overheat and become damaged.
- U. While on school grounds, devices are only to be used in classrooms or other designated areas.
- V. Store devices safely when they are not in use.
- W. Students must transport devices closed in their backpack, with the backpack completely zipped closed and with both shoulder straps secure on their shoulders.
- X. Students should seek parental or teacher approval before posting or sharing photos or video of other students.
- Y. You will have the same device next year, so protect it as if it were your own.
- Z. Enjoy this wonderful resource! You are among a select few students who attend school districts offering a device to every student. Limitless learning begins with you, so take advantage of this opportunity to excel academically and become a good “digital” citizen.

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 district-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 sleeve 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 school district or individual school names, logos, or trademarks 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 district settings on my device.
- I will immediately notify my teacher, the building level technology coordinator, or designee 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

- Dyer County 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.

If 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.

1:1 Website Additional information, details, and examples regarding the RUP and DCS technology resources and guidelines are found on the DC website.

1:1 Responsibilities/Policies

Policies

Technology made available to students and staff in the Dyer County Schools are provided to enhance learning and improve communication. The Board of Education has established policy to govern student and employee use of these resources. The use of school district technological resources on district-owned devices or personal devices, including access to the internet, is a privilege, not a right. Individual users of the school district's technological resources are responsible for their behavior and communications when using those resources. Responsible use of technological resources includes behaviors that are ethical, respectful, academically honest, and supportive of student learning. Students and staff are expected to learn and apply all applicable policies. All students and employees will be informed annually of the requirements of said policies and the ways to access or acquire a copy of the same. Students and staff will annually sign a statement indicating they understand and will strictly comply with these requirements.

Dyer County Schools' 1:1 Procedures and Guidelines are updated and maintained in the DCS Students Responsible Use Policy (RUP), DCS Employee RUP, and 1:1 Resource Guide. Copies of all these documents are available to parents and staff on the district website.

Students and legal guardians must sign the agreement of the Responsible Use Policy, known as the RUP, to use district-issued devices or any technology resources provided by the school district. During deployment, all students and guardians will become aware of the resource guide and will be asked to familiarize themselves with the content – using it as a ready online reference. A video will also be viewed at deployment – reiterating these details and requirements. If the RUP or contents of the 1:1 Resource Guide are not followed, disciplinary action and consequences will be enforced, up-to and including the loss of device access privileges or legal action.

Disclaimer

The board makes no warranties of any kind, whether express or implied, for the service it is providing. The board will not be responsible for any damages suffered by any user. Such damages include, but are not limited to, loss of data resulting from delays, non-deliveries or service interruptions, whether caused by the school district's or the user's negligence, errors, or omissions. Use of any information obtained via the internet is at the user's own risk. The school district specifically disclaims any responsibility for the accuracy or quality of information obtained through its internet services.

Rules for Use of School Technological Resources

1. School district technological resources are provided for school-related purposes only.

Acceptable uses of such technological resources are limited to responsible, efficient, and legal activities that support learning and teaching. Use of school district technological resources for political purposes or for commercial gain or profit is prohibited. Student personal use of school district technological resources for non-educational purposes is also prohibited. The board permits infrequent and brief personal use by employees during personal time, provided that it does not interfere with school district business and is not otherwise prohibited by board policy or procedure.

2. School district technological resources are installed and maintained by the Director of Schools or designee. Students and employees shall not attempt to perform any installation or maintenance without the permission of the building-level technology coordinator.

3. Under no circumstance may software purchased by the school district be copied for personal use.

4. Students and employees must comply with all applicable laws, including those relating to copyrights and trademarks, confidential information, and public records. Any use that violates state or federal law is strictly prohibited. Plagiarism of internet resources will be treated in the same manner as any other incidents of plagiarism.

5. No user of technological resources, including a person sending or receiving electronic communications, may engage in creating, intentionally viewing, accessing, downloading, storing, printing or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages or other material that is obscene, defamatory, profane, pornographic, harassing, abusive, or considered to be harmful to minors. All users must comply with policy 6.304 (Student Discrimination, Harassment, Intimidation, Bullying, and Cyberbullying) when using school district technology.

6. The use of anonymous proxies to circumvent content filtering is prohibited. DCS is not responsible for content accessed by bypassing safeguards that are in place.

7. Users may not install or use any internet-based file sharing program designed to facilitate sharing of copyrighted material.

8. Users of technological resources may not send electronic communication fraudulently (i.e., by misrepresenting the identity of the sender).

9. Users must respect the privacy of others. When using Email, chat rooms, blogs, or other forums of electronic communication, students must not reveal personal identifying information, or information that is private or confidential, such as the home address or telephone number, credit or checking account information or social security number of themselves or fellow students. School employees will follow FERPA guidelines relating to student information and media release.

10. Users may not intentionally or negligently damage computers or other devices, computer systems, accessories, software, computer networks, or data of any user connected to school district technological resources. Users may not knowingly or negligently transmit computer viruses or self-replicating messages or deliberately try to degrade or disrupt system performance.

11. Users may not create or introduce games, network communications programs, or any foreign program or software onto any school district electronic device or network without the express permission of the Director of Schools or designee.
12. Student users are prohibited from using another individual's user ID or password for any technological resource.
13. Users are prohibited from engaging in unauthorized or unlawful activities, such as "hacking" or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems, or accounts.
14. Student users may not read, alter, change, block, execute, or delete files or communications belonging to another user.
15. Users shall only access data systems or subscriptions that are currently approved by DCS.
16. If a user identifies a security problem on a technological resource, he or she must immediately notify the building level technology contact or designee. Users must not demonstrate the problem to other users. Any user identified as a security risk will be denied access.
17. Teachers and other staff shall make reasonable efforts to supervise students' use of the Internet during instructional time, to ensure that such use is appropriate for the student's age and the circumstances and purpose of the use.
18. Views may be expressed on the internet or other technological resources as representing the view of the school district or part of the school district only with prior approval by the Director of Schools or designee.
19. DCS does not back up student files. In the event of computer failure, user data will not be recovered from the device hard drive. Users are responsible for storing and backing up their own data.
20. Those who use district owned and maintained technologies to access the Internet at home are responsible for both the cost and configuration of such use.
21. DCS may provide students with a closed-campus Email account. Users are expected to communicate with the same appropriate, mindful, and courteous conduct online as offline. Email usage may be monitored and archived. There is no expectation of privacy with school Email accounts. Willful misuse may result in disciplinary action and/or criminal prosecution under applicable state and federal law.

Electronic Mail (Email) guidelines

- Basic rules to be observed when using Email include:
- Use for official business only
- Do not interrupt instructional time sending or receiving Email
- Email intended for distribution to all school employees is restricted to principals (or designee)
- Email intended for distribution to all employees in the district is restricted to designated central office staff only

Network Publishing

Content published via the Dyer County Schools network (both the Internet and the Intranet) must comply with the following regulations:

- All publications must comply with all policies and regulations of the district and all state, federal and international laws concerning copyright, intellectual property and use of devices.
- All DCS publications should reside on the district's network. Any exceptions must be approved by the Director of Schools or designee.
- All publications must provide a link to the Dyer County Schools home page.
- All district websites must include the statement, "Dyer County Schools does not discriminate in its programs or employment on the basis of race, color, religion, national origin, handicap/disability, sex or age."
- All publications must be reviewed and approved by the school district for distribution or posting.
- Design of the district website is the responsibility of the Director of Schools or his/her designee. Other publications intended for the public may be designed and developed by individuals or groups of employees with permission of appropriate management staff.

Web Applications

- DCS teachers are constantly seeking new tools and resources to enhance the student learning experience. Certain applications require parental permission for the use of sites, based on age and other terms. Staff will follow all contractual terms and federal guidelines – seeking parental permissions as needed.

Digital Citizenship

Rationale

Dyer County Schools (DCS) believes that all students should be adequately educated to function as citizens in an increasingly digital world. To this end, DCS uses free and purchased resources to train students regarding the technology skills, digital literacy skills, and digital citizenship skills they will need to succeed in college, in their careers, and in their relationships with other digital citizens. DCS strives to remain current and well-educated in new technologies helping learners understand how to use new technology successfully and appropriately. DCS allows families to determine the parameters for time spent on or off devices, and DCS supports parental decisions about the degree of technology use inside their homes. DCS also recognizes the need for digital health and wellness education and strives to help students maintain a healthy balance between online activities and relationships with the other activities and relationships in their lives. Students are to follow all provisions of the DCS Responsible Use Policy (RUP) at all times.

Curriculum

DCS utilizes free tools through Common Sense Media (scope and sequence provided at <https://www.commonsensemedia.org/educators/scope-and-sequence>) to train students about various aspects of digital citizenship. These tools are used in Kindergarten through 12th grade and include topics such as Internet Safety, Privacy and Security, Relationships and Communications, Cyberbullying, Digital Footprint and Reputation, Self-Image and Identity, Information Literacy, Creative Credit and Copyright.

Parent Resources

DCS believes that all educators and parents can and should help educate students about these key skills. DCS encourages parents to access quality parent training resources using any of the following sources:

- Netsmartz (Grades K-8) <http://www.netsmartz.org/Parents> includes videos, resources, and advice for parents to help them know how to talk to students about various digital citizenship topics and concerns.
- Common Sense Media (Grades K-8) <https://www.commonsensemedia.org/parent-concerns> includes age-appropriate guidelines for families plus videos and articles to help with tough conversations.
- Common Sense Media also provides family tips about social media, body image, digital footprint, photo sharing, sexting, cyberbullying, privacy, and online imagery.
- https://www.commonsensemedia.org/sites/default/files/uploads/connecting_families/tip_sheets_all.pdf
- Learning.com (Grades K-7) includes an online safety guide containing definitions, tools, tips, and resources concerning digital etiquette, filtering, virus protection, and privacy.
- [HTTP://WWW.LEARNING.COM/RESOURCES/PDF/PRODUCTS/PARENTS/PARENT_ONLINE_SAFETY_GUIDE_EN.PDF](http://WWW.LEARNING.COM/RESOURCES/PDF/PRODUCTS/PARENTS/PARENT_ONLINE_SAFETY_GUIDE_EN.PDF)
- FBI Safe Online Surfing Modules (Grades 3-8, PCs only) <HTTPS://SOS.FBI.GOV/> include interactive games to teach students to be safe and responsible in their digital activities and interactions.

Copyright

DCS believes that all students should be adequately educated to function as citizens in an increasingly digital world. To this end, DCS makes understanding and applying copyright guidelines part of our K-8 digital citizenship curriculum and expects all students and staff to use best practices with regards to copyright guidelines.

First, DCS recognizes that federal law states that it is illegal to duplicate or distribute copyrighted materials without authorization of the holder of the copyright, except for certain exempt purposes. Copyright laws govern the use of copyrighted materials. Teachers and students may use copyrighted materials for educational projects and learning activities, but they must follow specific “fair use” guidelines. Staff and students receive copyright and fair use instruction and/or guidelines from a variety of sources, including:

- Common Sense Media. Vertically and horizontally aligned copyright lessons for students K-7 include “A Creator’s Rights,” “A Creator’s Responsibilities,” “Copyrights and Wrongs,” “Rework, Reuse, Remix,” “How to Cite a Site,” “Whose is it, Anyway,” and “My Creative Work.” Because copyright laws are complex, DCS works to help students learn to analyze each situation and make educated judgments on a case-by-case basis.
- ELA Classes. State English/Language Arts standards include instruction on when and how to cite sources when using copyrighted material in student work.
- District Copyright Guidance: White paper

Collaboration and Social Networking

Collaboration and social networking have become vital parts of a student’s education. Online networking connects people in order to form virtual communities. Users must respect the privacy of others. When using Email, chat rooms, blogs, or other forums of electronic communication and collaboration, students must not reveal personal identifying information or information that is private or confidential. Online behavior should be appropriate and follow the guidelines set forth by the DCS RUP. When any student’s online behavior has a direct and immediate effect on school safety or maintaining order and discipline in the schools, the student may be disciplined in accordance with board policy.

Best Practices for Student Use of Social Media

- Don't share personal/private information such as identifying information or passwords with peers.
- Only accept friend requests/followers from people you know.
- Don't post anything you wouldn't want your parents, teachers, or employer (current or future) to see.
- Assume everything you write online will become public.
- Be real – the real you is better than anything you might pretend to be.
- Be respectful of the opinions of others in your posts or comments.
- Remember you are responsible for the content you post.
- Learn about privacy settings and review them often. DCS may use any means available to request the removal of information on personal websites or social media sites that substantially disrupts the school environment. DCS 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.

Digital Etiquette

DCS also encourages students to use appropriate digital etiquette (commonly referred to as netiquette) when interacting with others in an online environment. The following links include helpful resources for parents and students regarding digital etiquette: <https://www.common sense media.org/blog/7-rules-to-teach-kids-online-etiquette>.

Student / Parent Responsibilities

Parent / Student Responsibilities Form Enclosed at the bottom of this page. Parents and students of grades/classes scheduled to receive chromebooks are required to attend one of the parent / student meetings before receiving a chromebook. The meetings will be announced and repeated to offer convenient times and locations. Parents will be notified in writing by the school office of meeting information.

Student Responsibilities

Students are responsible for the general care of the Chromebook and carry case they have been issued by the school district.

1. Dyer County Schools owned and issued Chromebooks are monitored and supported by the Office of Technology 24/7.
2. Chromebooks that are broken or fail to work properly must be taken to the school's media center / library as soon as possible.
3. District owned Chromebooks should never be taken to an outside computer service for any type of repairs or maintenance.
4. Students should never leave their Chromebooks unattended except locked in their school locker.
5. Students must pass our Chromebook safety and usage test of a score of 95% or higher.
6. Students are required to keep their device in the provided case anytime they are walking with the Chromebook outside of the classroom. (Example- hallway, bus, cafeteria, etc.)

General Precautions

1. No food or drink should be next or near the Chromebook.
2. Cords, cables, and removable storage devices must be inserted carefully into Chromebooks.
3. Chromebooks should not be used or stored near pets.
4. Chromebooks should not be used with the power cord plugged in when the cord may cause a tripping hazard.
5. Chromebooks and provided cases must remain free of any writing, drawing, stickers, and labels. Students may clip tags to their cases, no more than 3 tags per case.
6. Chromebooks should arrive at school fully charged and ready to be used at school year day. (The device has a 10-hour battery life.)
7. Heavy objects should never be placed on top of Chromebooks, the Chromebook screen can be damaged if subjected to heavy objects, rough treatment, some cleaning solvents, and other liquids. The screens are particularly sensitive to damage from excessive pressure.

8. Do not put pressure on the top of a Chromebook when it is closed.
9. Do not store a Chromebook with the screen open.
10. Do not place anything in the protective case that will press against the cover.
11. Make sure there is nothing on the keyboard before closing the lid (e.g. pens, pencils, or disks).
12. Only clean the screen with a soft, dry microfiber cloth or antistatic cloth.

Asset Tags and Signed Student and Parent Permissions

1. All Chromebooks will be labeled with a District asset tag.
2. Asset tags may not be modified or tampered with in any way.
3. The signed student and parent permission document should remain on file in the school office at all times.

Dyer County Issued Case

1. Each student will be issued a protective case for his/her Chromebook that should be used whenever the Chromebook is being transported or not in use.
2. Although the cases are reinforced to help protect the Chromebooks, they are not guaranteed to prevent damage. It remains the responsibility of the student to care for and protect his/her device.
3. Chromebooks should always be carried in the district issued case.

Carrying Chromebooks

1. Always transport Chromebooks with care. Failure to do so may result in disciplinary action.
2. Never lift Chromebooks by the screen.
3. Never carry Chromebooks with the screen open.

DISTRICT COPYRIGHT GUIDANCE

INTRODUCTION As the Dyer County school district embarks on greater digital access to instructional resources and academic content, copyright protection and lawful management of copyrights within an educational setting has become an important topic of discussion and concern. Gone are the days when copyright was limited to requests submitted through the copy shop, plagiarism guidelines for students, and the selection of music and playwright agreements in the fine arts department. Today's educator is interested in following the law as it relates to Fair Use, online publishing, and what constitutes fairness for educational purposes. This white paper is an attempt to offer some guidance and resources to teachers and support staff facing copyright considerations in their work.

BACKGROUND The U.S. Copyright Office was created by Congress as part of the Library of Congress in 1897. In 2011, the Copyright Office employed 450 employees who processed more than 700,000 registration claims.

CONSTITUTIONAL PROTECTION: The Constitutional Provision Respecting Copyright. The Congress shall have Power...to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries. –United States Constitution, Article 1, Section 8

THE LAW: The Copyright Law of 1976 was enacted in 1976, as Pub. L. No. 94-553, 90 Stat. 2541, in chapters 1 through 8 and 10 through 12 of title 17 of the United States Code.

DEFINITION: Copyright is the legal right granted to an author, a composer, a playwright, a publisher, or a distributor to exclusive publication, production, sale, or distribution of a literary, musical, dramatic, or artistic work. Copyright laws are designed to protect a creator's right to be compensated and to control how his or her work is used. (Merriam-Webster)

PURPOSE: Copyright is a form of legal protection given to content creators through the assignment of specific rights to works that qualify for protection. In the United States, copyright protection exists from the time the work is created in a fixed, tangible form of expression. The copyright in the work of authorship immediately becomes the property of the author who created the work. A qualifying work is the expression, not the idea. In the U.S., registration of domestic works is required in order to sue for infringement. However, an author does not have to register a work, announce that the work is copyright protected, or display the copyright symbol to enjoy copyright protection. All he or she must do is create an original work in tangible form. Copyright law exists to foster creativity and spur the distribution of new and original works. Generally, unless your situation meets one of the exceptions outlined in the Copyright Law, you must get explicit permission from the copyright holder before you can lawfully reuse, reproduce or redistribute a copyright-protected work – even within the walls of your institution.

Section 110 of Copyright Law deals with use of materials in an educational setting.

FAIR USE: Fair use is primarily intended to allow the use of copyright-protected works for commentary, parody, news reporting, research and education. However, not all uses in an academic context are automatically considered fair use. According to the Copyright Law of 1976, the factors to be considered for Fair Use include (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes (2) the nature of the copyrighted work (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole and (4) the effect of the use upon potential market for or value of the copyrighted work.

CONFU: The Conference on Fair Use was established by the U.S. Department of Commerce to bring together copyright owners and user interests to discuss fair use issues that new technologies raise and to develop guidelines for fair use by librarians and educators. After two and a half years, the conference could not reach consensus. In 1996,

the Consortium of College and University Media Centers (CCUMC) convened to draft a set of fair use guidelines. These guidelines, while not legally binding, are a great resource to follow.

PROBLEM

Many institutions have adopted a policy of “when in doubt, obtain permission.” However, in education, the volume of work cited, referenced, used in research or reporting, can be tremendous. Likewise, one would not want to discourage students from board-based research and consideration of works that are copyrighted, where students seek use for education rather than commercial gain. In the past, teachers found themselves confined to a classroom and felt generally safe about calling fair use decisions. In a digital world, however, teachers no longer operate behind closed doors and must become knowledgeable practitioners of fair use. It is important that all staff who post online content or recommend online content for posting understand the importance of only citing works that have permission or fall within the guidelines for fair use or public domain.

SOLUTION We intend to be in compliance with the law as it relates to Copyright and Fair Use. Likewise, we wish to model practices for students that abide by the law and give consideration to those who create works worthy of citing or including in one’s research, writing, or study. As good (digital) citizens, we appreciate that it is in good taste to ask for permission to post or quote the work of others. It is unlikely a teacher will end up in court over an infringement - unless such infringement interferes with the owner’s potential income. Teachers should know how to ask for permission and should teach students to ask before using any material that might be in question. Most digital resources predate copyright law, but we all know that the internet is not in the public domain – so fair use would apply. In Education World (cited below), you’ll see this – “as a general rule, a good way to determine whether a multimedia resource is copyright protected or in the public domain is to relate it as closely as possible to a print resource.” Use caution with posting or copying links to sites with descriptions; downloading graphs, logos, fonts, photographs, or illustrations; using information from a site and making it sound like it is your own; bypassing advertising to “deep link” a site; or simply copying a site’s html code. Keep in mind that works cited on a site may not have all the proper permissions, so question your sources. Software use and licensing should be handled on a case-by-case basis, in coordination with administration and district technical staff.

- Copyright basics video (licensed by the Copyright Clearance Center)
http://www.copyright.com/content/cc3/en/toolbar/education/resources/copyright_basics1.html
- Copyright on Campus (licensed by the Copyright Clearance Center)
http://www.copyright.com/content/cc3/en/toolbar/education/resources/copyright_on_campus.html
- Using Course Management Systems – Guidelines and Best Practices for Copyright Compliance (published by the Copyright Clearance Center).
<http://www.copyright.com/content/dam/cc3/marketing/documents/pdfs/Using-CourseManagement-Systems.pdf>
- Campus Guide to Copyright Compliance for Academic Institutions – sourced from www.copyright.gov and published by the Copyright Compliance Center
<https://www.copyright.com/Services/copyrightoncampus/>

- Exceptions for the Use of Materials in an Educational Setting are covered in these online materials from the Copyright Compliance Center

https://www.copyright.com/Services/copyrightoncampus/basics/fairuse_edu.html .

- “Education World” offers a free online resource as a guide to copyright and fair use for educators.

http://www.educationworld.com/a_curr/curr280.shtml

- Resources for seeking permission:

- Written materials

- The Copyright Clearinghouse (www.copyright.com)

- [Icopyright \(http://info.icopyright.com/\)](http://info.icopyright.com/)

- Musical performances:

- [BMI \(www.bmi.com\)](http://www.bmi.com)

- [ASCAP \(www.ascap.com\)](http://www.ascap.com)

- Song reproductions:

- National Music Publishers’ Association (www.nmpa.org)

- Photographs:

- [Corbis \(www.corbis.com\)](http://www.corbis.com)

- [Time, Inc \(www.thepicturecollection.com\)](http://www.thepicturecollection.com)

- [Istockphoto \(www.istockphoto.com\)](http://www.istockphoto.com)

- Famous artwork:

- [Art Resource \(www.artres.com\)](http://www.artres.com)

- Cartoons:

- [The Cartoonbank \(www.cartoonbank.com\)](http://www.cartoonbank.com)

- If you know the author or the author is listed, you may contact them directly. Obtaining approval in writing is preferable, but verbal agreement (well documented) is better than none. Sending a letter of confirmation

from your office detailing the terms of the agreement and content of the conversation would be a good document to keep. ○ When requesting copyright permission, a lack of response from the copyright holder does not, under U.S. law, negate the need to obtain permission. Keep in mind that some works may contain multiple copyright holders and require permission from each.

Anyone can call the copyright office toll free at 1-877-476-0778. Contact information is also available via Email on the copyright.gov website.

Chapter 1000 of copyright law covers Websites and Website Content. Read the full text at <http://www.copyright.com/content/dam/cc3/marketing/documents/pdfs/Using-Course-Management-Systems.pdf>

CONCLUSION

It seems that teachers must look at copyright from two angles. First, to make sure students understand the importance and implications of non-compliance with the law and the spirit of the law that protects original work. Second, the teacher must also abide by Fair Use under the law and model due diligence for students, while protecting themselves and the school district. In addition to this paper, a list of examples, indicating what might be permissible and what might be in question, is available as a guide for the classroom. While copyright is a sometimes vague and elusive target, it is expected that teachers in the Dyer County Schools will make every effort to be acquainted with the law, to become a practitioner who upholds and models lawful behavior, and who questions use or misuse of copyright with others who work for the district, as well as students. The greatest defense for a possible infringement is to (1) always refrain from situations where you might limit potential financial gain of a copyright holder (2) keep your cited works, either online or in print, to a minimum quantity and update them regularly (3) add a disclaimer to your online resources indicating that you either have permission, are seeking permission, or are only using cited sources for educational purposes under Fair Use.

1:1 Resources

Visit the following links to find out how others are using one-to-one computing.

- <http://www.projectred.org/>

- Project RED conducted the first and only national study of education technology to focus on student achievement and financial implications. Project RED's research of nearly 1,000 schools discovered a replicable design for successfully introducing technology into the classroom — one that leads to improved student performance and cost benefits.

- <http://www.one-to-oneinstitute.org/>

- The One-To-One Institute provides information and resources to educators, school administrators and parents about one-to-one computing in schools. It is an international non-profit committed to "igniting 21st Century education through the implementation of one-to-one technology in K-12 education environments."

- <http://www.k12blueprint.com/>

- K-12 Blueprint offers resources for education leaders involved in planning and implementing technology initiatives. The website was developed by the Intel Corporation.

- http://www.educationworld.com/a_tech/tech/tech194.shtml

- Tech integration no longer means being stuck in a lab or a corner of the classroom. Find out how laptops and tablets are landing in the hands of so many students and "Get the 411" on laptops and tablets in the classroom.

- http://www.educationworld.com/a_tsl/archives/ed_tech.shtml

- Various links from Education World about how teachers from throughout the country incorporate technology into classroom lessons, from Ancient Egypt to Airplanes.

- <http://blogs.worldbank.org/edutech/1-to-1>

- Here are "10 comments on 1-to-1 computing in education" presented at world-wide gathering of education officials interested in rolling out prominent one-to-one computing initiatives.

- <http://www.iste.org/connect/iste-connects/blog.aspx>

- The ITSE Connects Blog is the official blog of the International Society for Technology in Education, and is a source of information on emerging education technology topics, tools and trends. ITSE is the premier membership association for educators and education leaders engaged in improving learning and teaching by advancing the effective use of technology in PK-12 and teacher education.

- <http://www.techlearning.com/article/7638>

- This article in the online education magazine Tech & Learning is about one-to-one computing and classroom management. It offers many tips on a variety of topics, from a "management by walking around" technique once practiced by President Theodore Roosevelt to test taking. The article includes links to other helpful resources.

- <http://blogs.worldbank.org/edutech/node/558>

- One-to-one computing isn't unique to Delavan-Darien schools. Such initiatives are happening all over the globe, in Argentina, Israel, Nepal, Rwanda, Spain and many other places. See where else with the links on this article.

- <http://www.maine.gov/mlti/>

- The state of Maine has a one-to-one program for middle and high school students, one of the first state-wide efforts of its kind in the US. In January 2010, the project has reached close to 30,000 middle schoolers and almost 24,000 high schoolers in more than 270 schools.

- <http://www.educatorstechnology.com/2013/06/the-5-important-elements-of-21st.html>

- Check out these five important elements of how the 21st Century Classroom is becoming the Digital Classroom.

- [Benefits of a Digitally Literate Community](#)

- This infographic shows some of the many benefits to having a digitally literate community. It's from the Colorado State Library system and was developed as part of "Project Encompass, a series of community meetings in Colorado focused on digital literacy and broadband adoption.

- <http://www.schrockguide.net/ipads-in-the-classroom.html>

- If you're a teacher and you use iPads in your classroom, you'll want to check this site out. Even if you aren't a teacher, you'll want to check this site out. Tons of resources and information about different apps and how they can be used for classroom learning.

1:1 Chromebook Repair Costs

Replacement costs for the Chromebooks are as follows:

Lenovo N42

Chromebook:	\$225.00
Power Supply:	\$30.00
Chromebook Screen	\$50.00
Protective Sleeve:	\$20.00
Keyboard upper case	\$50.00

Lenovo 14e

Power Supply:	\$30.00
Chromebook Screen	\$120.00
Protective Sleeve:	\$30.00

Authorized Use Policy

A. Introduction It is the policy of the District 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 District 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 District 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

Access to electronic research requires students and employees to maintain consistently high levels of personal responsibility. The existing rules found in the District's Behavioral Expectations policy (Board Policy/Regulation 2610) as well as employee handbooks clearly apply to students and employees conducting electronic research or communication.

One fundamental need for acceptable student and employee use of District 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 and employees utilizing electronic resources to conduct research or complete work.

These passwords/account codes shall not be shared with others; nor shall students or employees 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 District 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 District technology and electronic resources is a privilege, which may be revoked at any time. Staff and 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 and employees may not claim personal copyright privileges over files, data or materials developed in the scope of their employment, nor may students or employees 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 and staff 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 and employees 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 or employees who engage in "hacking" are subject to loss of privileges and District 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 District, a business, or any other governmental agency obtained through unauthorized means.

To the maximum extent permitted by law, students and employees 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 District and school administration reserve the right to remove files, limit or deny access, and refer staff or students violating the Board policy to appropriate authorities or for other disciplinary action.

Privileges

The use of District technology and electronic resources is a privilege, not a right, and inappropriate use will result in the cancellation of those privileges. All staff members and 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 and employees 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 system 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 District permits staff and 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 and staff members must sign the District's "Technology User Consent Form" and submit the signed Form to the District. If the District 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 District does not provide technical support for personal technology devices.
3. Students and staff will access the District's wireless Internet network with the username and login provided to them and assigned to them by the District; students and staff 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 District is not responsible for the damage, loss, or theft of any personal technology device.
6. The District 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 District 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 and staff members 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, staff and 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 District, or behaves in such a way that the service or security of the District is degraded, the District reserves the right to permanently disconnect that device from the District'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 District 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 District's policies, procedures or rules, or engaged in other misconduct while using the personal technology device. Violation of the District's policies or local, state and/or federal laws will result in revocation of the privileges given under this regulation.

13. The District 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 District's wireless network. By logging onto or accessing the District's wireless network, staff and students are agreeing to the above listed conditions. In the event that a student or staff member uses the District'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 District utilizes computer software applications and web-based services operated not by the District 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 District 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 District 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 District 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 District to provide personal information to third party operators. No personal student information is collected for commercial purposes. The District'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 District Email address until such time as the student is no longer enrolled with the District.

Services

While the District is providing access to electronic resources, it makes no warranties, whether expressed or implied, for these services. The District 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 District specifically denies any responsibility for the accuracy of information obtained through Internet services.

Security

The Board recognizes that security on the District'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 District 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 District 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 District 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 District electronic network or technology system will result in the immediate loss of computer service, disciplinary action and, if appropriate, referral to law enforcement officials.

Consequences

The consequences for violating the District'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
9. Employee disciplinary action up to and including dismissal.

Authorized Usage TECHNOLOGY USER CONSENT FORM

Student Consent

I have read and understand the Dyer County School District's 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 the Dyer County School District's 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 students 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 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 Email Agreement

My signature below signifies my understanding that Dyer County Schools Email accounts are for educational purposes only and provided as a privilege by Dyer County Schools. Any misuse of the Dyer County School 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 Dyer County Schools, 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 Dyer County 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.

Student Signature: _____ **Date:** _____

Parent Signature: _____ **Date:** _____

Dyer County Schools Student Email accounts are provided through Google G Suite for Education.

Please complete the form below. Make any needed additions and/or corrections.

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

Student ID: _____

Grade: _____

_____ Student Last Name, First Name

Student Equipment Agreement Form

Student ID: _____ School Year: _____

Last Name: _____ First Name: _____

DCS 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 DCS 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.

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

1. I will take care of my chromebook as identified in the Dyer County Schools 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 are responsible and appropriate, meet DCS expectations and are educational.
9. I will not place decorations (such as labels, stickers, marker, 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 District. 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 is inappropriate content is found on the device.
13. I agree to return the District 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.

To Be Completed by STUDENT:

First & Last Name

(print): _____ Grade: _____

Signature: _____

Date: _____

To be Completed by PARENT/GUARDIAN:

First & Last Name (print): _____ Relationship: _____

Address: _____

City: _____ State: _____ Zip Code: _____

Email Address: _____ (Home Phone): _____

(Cell): _____ (Work): _____

Parent Signature: _____

Date: _____

RUP AND WEB APPLICATIONS GUIDE

SIGNATURE PAGE.

Legal ownership of the device belongs to Dyer County Schools (DCS). The student's right to use and possess the device is terminated upon withdrawal from Dyer County Schools. The failure to timely return the property and the continued use of it for non-school purposes without the school system's consent will be considered unlawful appropriation or theft of the school system's property. If the device is intentionally or negligently damaged, lost, or stolen, the student/parent is responsible for the cost of repair, current replacement cost of the device, or its fair market value. Loss or theft of the device must be reported to the DCS District by the next school day. Payment for broken, lost or stolen devices shall be under terms reasonably agreed upon between DCS and the parents. In the event DCS has to resort to legal action to recover an electronic device or payment for damage, destruction, loss or theft of such a device from parent(s) or guardian(s) of a student, the undersigned parent or guardian agrees to pay the reasonable attorney's fees and costs of DCS incurred in such effort. As the parent/guardian, my signature indicates I agree to abide by the conditions listed in the DCS Responsible Use policy (RUP) as well as the content provided on the 1:1 Website. Failure to honor the terms of this Policy may result in the denial of Internet and other electronic media accessibility. Furthermore, the student may be subject to disciplinary action, and, if applicable, the device may be recalled. I give my permission for my child to have access to the described electronic resources and have access to the Internet, including an Email account.

Parent/Guardian Name (please print): _____

Date: _____

Parent/Guardian Signature: _____

As the student, my signature indicates that I have received, read, and agree to follow the DCS Responsible Use Policy and have been made aware of and intend to follow the full 1:1 Website. I agree to the terms and conditions outlined and in return will have conditional access to the described electronic resources, including an Email account.

Student Name (please print): _____ Date: _____

Student Signature: _____

Student Grade: _____