Acceptable Use Policy
Corinth School District

The purpose of this policy is to provide clear guidelines and regulations regarding the safe, legal, considerate and responsible use of this technology, as well as all technological resources utilized by students, staff, parents, and volunteers of the Corinth School District. All Corinth School District technological resources and information stored on them are governed by district policies and are subject to school supervision and inspection. This policy applies regardless of whether such use occurs on or off school district property, and it applies to all school district technological resources, including but not limited to computer networks and connections, the resources, tools and learning environments made available by or on the networks, and all devices that connect to those networks.

The Corinth School District reserves the right to monitor, access, retrieve, read and disclose all messages, information, and files which have been created, sent, posted from, stored on, or utilized by its technological resources to law enforcement officials and others without prior notice. Any individual who violates this policy or any applicable local, state or federal laws is subject to disciplinary action, a loss of technology privileges and may face legal action.

A. EXPECTATIONS FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

Students, staff, may only use school district technological resources and others expressly authorized by the school district. The use of school district technological resources, 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 school district technological resources is use that is ethical, legal, respectful, academically honest and supportive of student learning. Each user has the responsibility to respect others in the school community and on the Internet. Users are expected to abide by the generally accepted rules of network etiquette. General student and employee behavior standards, including those prescribed in applicable board policies, the Student and Employee Handbook and other regulations and school rules, apply to use of the Internet and other school technological resources.

In addition, anyone who uses school district computers or electronic devices or who accesses the school network or the Internet using school district resources must comply with the additional rules for responsible use listed in Section B, below. These rules are intended to clarify expectations for conduct, but should not be construed as all- inclusive.

All students and employees must be informed annually of the requirements of this policy and the methods by which they may obtain a copy of this policy. Before using school district technological resources, students and employees must sign a statement indicating that they understand and will strictly comply with these requirements. Failure to adhere to these requirements will result in disciplinary action, including revocation of user privileges. Willful misuse may result in disciplinary action and/or criminal prosecution under applicable state and federal law.

B. RULES FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

1. School district technological resources are provided for school-related purposes only during school hours. 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.
2. School district technological resources are installed and maintained by members of the Technology Department. Students and employees shall not attempt to perform any installation or maintenance without the permission of the Technology Department.
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 cheating, as stated in the Student Handbook.
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 all student handbook and district policies regarding Student Bullying, Harassment, Threat, Violence and Assault, when using school district technology.
6. The use of anonymous proxies to circumvent content filtering is prohibited.
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 communications fraudulently (i.e., by misrepresenting the identity of the sender).
9. Users must respect the privacy of others. When using e-mail, chat rooms, blogs or other forms 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. In addition, school employees must not disclose on school district websites or web pages or elsewhere on the Internet any personally identifiable, private or confidential information concerning students (including names, addresses or pictures) without the written permission of a parent or guardian or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA). Users also may not forward or post personal communications without the author's prior consent.
10. Users may not intentionally or negligently damage computers, computer systems, digital or electronic devices, 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. Users must scan any downloaded files for viruses.
11. Users may not create or introduce games, network communications programs or any foreign program or software onto any school district computer, electronic device or network without the express permission of the director of technology or designee.
12. 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.
13. Users are prohibited from using another individual's ID or password for any technological resource without permission from the individual. Students must also have permission from the teacher or other school official.
14. Users may not read, alter, change, block, execute or delete files or communications belonging to another user without the owner's express prior permission.
15. Employees shall not use passwords or user IDs for any data system for an unauthorized or improper purpose.

16. If a user identifies a security problem on a technological resource, he or she must immediately notify a system administrator. Users must not demonstrate the problem to other users. Any user identified as a security risk will be denied access.
17. Teachers 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. No comments or pictures may be placed on the Internet or other technological resources representing the view of the school or school district without prior approval of the superintendent or designee.
19. Without permission by the Board, users may not connect any personally-owned technologies such as laptops and workstations, wireless access points and routers, etc. to district owned and maintained networks. Connection of personal devices such as iPods, smartphones, digital tablets and printers is not permitted. The board is not responsible for the content accessed by users who connect to the Internet via their personal mobile telephone technology (e.g., 3G, 4G service).
20. Users must back up data and other important files regularly.
21. 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.
22. Students who are issued district owned and maintained laptops must also follow these guidelines:
    a. Keep the laptop secure and damage free.
    b. Use the provided protective book bag style case at all times.
    c. Do not loan out the laptop, charger or cords.
    d. Do not leave the laptop in your vehicle.
    e. Do not leave the laptop unattended.
    f. Do not eat or drink while using the laptop or have food or drinks in close proximity to the laptop.
    g. Do not allow pets near the laptop.
    h. Do not place the laptop on the floor or on a sitting area such as a chair or couch.
    i. Do not leave the laptop near table or desk edges.
    j. Do not stack objects on top of the laptop.
    k. Do not leave the laptop outside.
    l. Do not use the laptop near water such as a pool.
    m. Do not check the laptop as luggage at the airport.
    n. **Back up data and other important files regularly. The Corinth School District will at times perform maintenance on the laptops by imaging and other support-related services. All files not backed up to a storage device will be deleted during this process. Keep a personal backup of all files for data retrieval.**

B. RESTRICTED MATERIAL ON THE INTERNET

The Internet and electronic communications offer fluid environments in which students may access or be exposed to materials and information from diverse and rapidly changing sources, including some that may be harmful to students. The Board recognizes that it is impossible to predict with certainty what information on the Internet students may access or obtain. Nevertheless school district personnel shall take reasonable precautions 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. The superintendent shall ensure that technology protection measures are used and are disabled or minimized only when permitted by law and board policy. The board is not responsible for the content accessed by users who connect to the Internet via their personal mobile telephone technology (e.g., 3G, 4G service).

C. 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 parent or guardian 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 monitoring of the student's e-mail 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 educational goals. Parental permission will be obtained when necessary to create and manage such third party accounts.

D. 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 superintendent may review files, monitor all communication and intercept e-mail messages to maintain system integrity and to ensure compliance with board policy and applicable laws and regulations. School district personnel shall monitor online activities of individuals who access the Internet via a school-owned computer or district-owned equipment. Under certain circumstances, the board may be required to disclose such electronic information to law enforcement or other third parties, for example, as a response to a document production request in a lawsuit against the board, as a response to a public records request or as evidence of illegal activity in a criminal investigation.

E. SECURITY/CARE OF PROPERTY

Security on any computer system is a high priority, especially when the system involves many users. Employees are responsible for reporting information security violations to appropriate personnel. Employees should not demonstrate the suspected security violation to other users. Unauthorized attempts to log onto any school system computer on the board's network as a system administrator may result in cancellation of user privileges and/or additional disciplinary action. Any user identified as a security risk or having a history of problems with other systems may be denied access. Users of school district technology resources are expected to respect school district property and be responsible in using the equipment. Users are to follow all instructions regarding maintenance or care of the equipment. Users may be held responsible for any loss or damage caused by intentional or negligent acts in caring for computers while under their control. The school district is responsible for any routine maintenance or standard repairs to school system computers.

F. PERSONAL WEBSITES/SOCIAL MEDIA

The district recognizes the use of online social media networks as a communications and e-learning tool. As a result, the district provides password-protected, innovative social tools for e-learning and collaboration purposes. However, public social media networks may not be used for classroom instruction without prior consent of the superintendent. The use of social media for personal use during district (on-contract) time is prohibited. The district may use publicly available social media for fulfilling its responsibility for effectively communicating in a timely manner with the general public, through designated employees at the direction of the board.

The superintendent may use any means available to request the removal of personal websites that substantially disrupt the school environment or that utilize school district or individual school names, logos or trademarks without permission.

1. 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 student may be disciplined in accordance with board policy.

2. Employees

All employees are to maintain an appropriate, professional relationship with students at all times. Employees' personal websites and social media posts, displays or communications must comply with all state and federal laws and any applicable district policies, including the Mississippi Educator Code of Ethics and Standards of Conduct which requires professional, ethical conduct.

3. Volunteers

Volunteers are to maintain an appropriate relationship with students at all times. A volunteer is encouraged to block students from viewing personal information on the volunteer's personal websites or online networking profiles in order to prevent the possibility that students could view materials that are not age-appropriate. An individual volunteer's relationship with the school district may be terminated if the volunteer engages in inappropriate online interaction with students.

G. FEDERAL ACCOUNTABILITY

The Corinth School District in order to be eligible for Federal Funds is required to incorporate and comply with both CIPA and COPPA requirements into the district's Acceptable Use Policy.

Children's Internet Protection Act (CIPA)

CIPA requires that schools and libraries that receive specific Federal Funds must certify to the funding agency that they have an Internet Safety Policy in place. Such a policy should use technology that blocks access to obscenity, child pornography, or material harmful to minors. It may also include monitoring of children as they are online. Congress wants the Internet Safety Policy to address hacking, chat rooms, email safety, disclosure of personal information concerning children, and unlawful activities of children online. CIPA became effective on April 21, 2001. Additionally, the Corinth School District, in accordance with the Broadband Data Improvement Act (BDIA) of 2008, is implementing a policy addressing cyberbullying and other social networking issues.

Broadband Data Improvement Act (BDIA)

BDIA declares that the issue of Internet safety includes issues regarding the use of the Internet in a manner that promotes safe, online activity for children, protects children from cybercrimes, including crimes by online predators, and helps parents shield their children from material that is inappropriate for minors. BDIA amends the Communications Act of 1934 to require elementary and secondary schools with computer access to the Internet to educate minors about appropriate online behavior, including online interaction with other individuals in social networking websites and in chat rooms and cyber bullying awareness and response.

H. 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.

User Application/Contract: I certify that I have read the Corinth School District's Acceptable Use Policy (AUP). I understand and agree to follow the above Terms and Conditions for the District's Internet use. I understand any violation of the District's Internet AUP will result in the loss of Internet access and/or my user account; may result in the loss of school provided technology devices; may result in other disciplinary action; and may constitute a criminal offense. I agree to report any misuse of the Internet resources to my system administrator. I use the Internet entirely at my own risk and I hereby release the District from any claims arising from my use of the Internet. *Note: This agreement will be placed in the user's permanent file.*

User Name (please print):_____

User Signature: _____ Date: _____

PARENT or GUARDIAN: As the parent or guardian of this student, I have read the District's Acceptable Use Policy (AUP) and this contract. I understand that access to the Internet resources is designed for educational purposes. I understand that controversial material is available on the Internet and I permit my child to use the Internet despite this potential availability. I will not hold the District responsible for materials my child acquires on the network. My child uses the Internet at my child's own risk and at my own risk. I hereby release the District from any claim arising from my child's use of the Internet. I agree to report any misuse of the Internet resources to a District administrator. I accept full responsibility for supervision if and when my child's use is not in a school setting. I understand that my child's violation of the District's Internet AUP will result in the loss of Internet access and/or my child's user account; may result in the loss of school provided technology devices;may result in other disciplinary action; and may constitute a criminal offense. I hereby give my permission for my child to access the Internet and I give permission to the District to issue an account for my child. I certify that the information contained on this application is correct.

Parent / Guardian Name (please print): _____

Parent / Guardian Signature: _____ Date: _____

PLEASE NOTE: Although District policy forbids unauthorized users to access the Internet; the District cannot guarantee that students will not gain unauthorized access. The District is not liable for such unauthorized access.
