LOWNDES COUNTY
School District
CALEDONIA • NEW HOPE • WEST LOWNDES • CAREER TECH

INTERNET/NETWORK ACCEPTABLE USE POLICY

Use of the Lowndes County School District's network shall be solely for the purpose of facilitating the exchange of information for this district in the furtherance of education, research, and job-related activities. The network also supports the educational and instructional endeavors of students and employees of the Lowndes County School District.

The Lowndes County School District's network is a complex system of components structured to perform specific functions within the district. The network system requires centralized management to ensure seamless operation; consequently, no user shall be allowed to attach any peripheral to the network without prior written permission. This includes, but is not limited to, hubs/switches, network storage devices, network printers, servers of any kind, and computers not owned by this district.

Anyone who uses the Lowndes County School District's network must also abide by the guidelines established in COPPA and CIPA. CIPA (Children's Internet Protection Act 2000) states that filtering services will be utilized on all computers accessing the Internet in the Lowndes County School District. COPPA (Children's Online Privacy Protection Act 1998) states that users will not disclose, use, disseminate, or give personal and/or private information about him/her, minors, or any other persons. In accordance, this district will provide filtering software for every internet accessible computer, and no employees shall disclose personal information about students on the district or school websites.

The following are examples of other inappropriate activities related to The Lowndes County School District's network, e-mail system, and the internet. Failure to abide by any of the district's internet/network "acceptable use" regulations shall result in suspension of the internet and email account. Violations are not limited to those listed below:

- Downloading, installing, or copying software of any kind onto a workstation or any network drive without approval of district personnel.
- Violating copyright laws.
- Damaging computer systems or computer networks (This includes changing workstation configurations such as printers, BIOS information, passwords, etc.)
- Accessing inappropriate web sites (sites containing information that is violent, illegal, sexual, etc.)
- Plagiarism of materials that are found on the internet.
- Sharing passwords.
- Broadcasting network messages by participating or sending chain email.
- Intentionally wasting limited resources such as disk space and printing capacity.
- Listening to radio or TV broadcasting on the internet.

Any violation of these guidelines may result in disciplinary action.

All users should realize when they use the internet, they enter a global world, and any actions taken by them will reflect upon the Lowndes County School District as a whole. As such, all users must behave in an ethical and legal manner and abide by the netiquette rules of network.

Each student utilizing the internet and his/her parent shall sign the district's "Internet/Network Usage Agreement Form" before being allowed to use the internet or network. All employees and community guests must also sign the district's applicable form before using the internet or network.

The Lowndes County School District's Board of Trustees has implemented the 1:1 Digital Learning Initiative, called Engaged Learning Initiative (ELI), an innovative plan focused on enhancing academic learning through new technology resources. As such, the district provides its students and staff access to a variety of technological resources, including laptops, MacBook, and IPads.

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 Lowndes County School District. All Lowndes County School District technological resources and information stored on the devices 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 Lowndes County 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

School district technological resources may only be used by students, staff, and others expressly authorized by the Technology Department. 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 for 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

- 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. All users' use of school district technological resources for amusement or entertainment may only occur during non-school hours.
- 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.

- Under no circumstance may software purchased by the school district be copied for personal use.
- Students and employees must comply with all federal, state, local, and 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.
- 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 that governs bullying, cyberbullying, and harassment when using school district technology and or networks.
- The use of anonymous proxies to circumvent content filtering is prohibited.
- Users may not install or use any internet-based file-sharing program designed to facilitate sharing of copyrighted material.
- Users of technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender; hacking another user's account).
- Users must respect the privacy of others. When using e-mail, chat rooms, blogs or other forms of electronic communication, users 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 users.
- School employees must not disclose on school district websites or web pages or elsewhere on the internet any personal 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) or policy JRAB, Compliance with FERPA. Users also may not forward or post personal communications without the author's prior consent.
- 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.
- 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.
- 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.
- 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. Supervisors can submit in writing a request to the Superintendent to access their employee's files.
- Users may not read, alter, change, block, execute or delete files or communications belonging to another user without the owner's express prior permission. Upon separation the district has the authority and all rights to delete or keep all said files.
- Employees shall not use passwords or user IDs for any data system for an unauthorized or improper purpose.
- 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.
- 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.

- Users may connect any personally-owned mobile devices to district owned and maintained networks. The board is not responsible for the content accessed by users who connect to the internet via their personal mobile technology (e.g., 3G, 4G service).
- Users must back up data and other important files regularly.
- 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.
- Users who are issued district owned and laptops, MacBooks, IPads, and other mobile technology must also follow these guidelines:
    - ✓ Keep the items secure and damage free.
    - ✓ Use the provided protective coverings case at all times.
    - ✓ Do not loan out the any items such as chargers or cords.
    - ✓ Do not leave the items in your vehicle.
    - ✓ Do not leave the items unattended.
    - ✓ Do not eat or drink while using the items or have food or drinks in close proximity to the items.
    - ✓ Do not allow pets near the items.
    - ✓ Do not place the items on the floor or on a sitting area such as a chair or couch.
    - ✓ Do not leave the items near table or desk edges.
    - ✓ Do not stack objects on top of the mobile device.
    - ✓ Do not leave the items outside.
    - ✓ Do not use the items near water such as a pool.
    - ✓ Do not check the items as luggage at the airport.

The District will at times perform maintenance on the MacBook's/IPads by imaging and other support-related services. All files not backed up to server storage space or other storage devices will be deleted during this process. Keep a personal backup of all files for data retrieval.

C. 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 technology (e.g., 3G, 4G service).

D. 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.

E. 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.

F. 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.

G. PERSONAL WEBSITES/SOCIAL MEDIA

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.

H. FEDERAL ACCOUNTABILITY

The Lowndes County 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. Anyone who uses the Lowndes County School District network must abide by the guidelines as established in COPPA and CIPA.

Children's Internet Protection Act (CIPA)

CIPA (Child Internet Protection Act 2000) states that filtering services will be utilized on all computers accessing the internet in the Lowndes County School District. CIPA requires that schools receiving federal funds, including E-rate, and Title II of the Elementary and Secondary Education Act, put into place internet security policies. Recognizing that no filtering software or appliances is 100% effective, the technology team will monitor and do as much as possible to keep the network and internet secured. 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.

Children's Online Privacy Protection Act (COPPA)

COPPA (Children's Online Privacy Protection Act 1998) states that users will not disclose, use, disseminate, or give personal and/or private information about him/her, minors or any other persons. COPPA requires commercial website managers to get parental consent before collecting any personal information from children under 13. Parents will have to sign a parental consent form to post their child's picture on school websites.

I. 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.

J. VIOLATIONS

Violations of policy will result in the following disciplinary actions.

- 1st offense – lose device for three days and will contact parents
- 2nd offense – lose device for five days and will contact parents
- 3rd offense – lose device for ten days and will contact parents
- 4th offense – lose device for six months excluding holidays/summer vacations and will contact parents