

Lee County School District Internet Acceptable Use Agreement for Employees

The Lee County Board of Education (LCBOE) recognizes the importance of increasing access to technological learning opportunities available to students and staff. The LCBOE believes that this increases the potential to support curriculum and student learning in facilitating resource sharing, innovation, and communication. As resources permit, informational technology services shall be made available in schools.

The School District (hereafter “District”) provides employees with electronic access including, but not limited to, an email system, a network connection, and Internet/Intranet access. The District also provides technology equipment including but not limited to desktop computers, laptop computers, iPads, cell phones, cameras, fax machines, and telephones. This Agreement governs all use of the District’s network, Internet/Intranet access, email systems and technology equipment. Personal technology equipment or personal email accounts that access or use the District’s network and the District’s Internet/Intranet access are subject to this Agreement.

Use of the Network and the Internet is a privilege, not a right. Use of Network and Internet access extends throughout an employee’s term of employment. The District reserves the right to suspend access at any time, without notice, for technical reasons, possible rule violations, security or other concerns.

Network and Internet access and technology equipment are provided as tools for District operations. The District reserves the right to monitor, inspect, copy, review, and store at any time, without prior notice, any and all usage of the Network and the Internet, as well as any and all materials, files, information, software, communications, and other content transmitted, received or stored in connection with this usage. All such information, content, and files are the property of the District. An employee shall have no expectation of privacy regarding them. Network administrators may review e-mails or files and intercept communications for any reason, including but not limited to, maintaining system integrity and ensuring employees are using the system consistent with this Agreement. The District reserves the right to disclose (release) text, images, or technology equipment to law enforcement agencies or appropriate third parties without the employee’s consent.

District personnel shall take all available precautions to restrict access to controversial materials, while recognizing that it is impossible to control all material which might inadvertently be discovered by users on a global network. Inappropriate and/or illegal interaction with the information service is strictly prohibited.

By virtue of using District technology, employees are subject to the provisions of this acceptable use agreement. If any user violates these provisions, access to the information service may be denied and the user may be subject to disciplinary action.

Terms of Internet Usage

1. User Responsibility – District employees accept responsibility for reporting any misuse of the network to their supervisor. Misuse may come in many forms, but is commonly viewed as any message(s) sent or received that indicates or suggest pornography, unethical or illegal solicitation, racism, sexism, inappropriate language, and other issues described below.
2. Assigned Employee Account - The use of assigned employee accounts must be in support of education and research aligned with educational goals and objectives of the District. Employees are personally responsible for the following provisions at all times when using the electronic information service:
 - Use of other organization’s networks or computing resources must comply with rules appropriate to that network.
 - Transmission of any material in violation of any law, rule or regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret.
 - Use of commercial activities by for-profit institutions is generally not acceptable.
 - Use of product advertisement or political lobbying is also prohibited.
3. Prohibited Activities – Employees are prohibited from using the District’s email system, network, or Internet/Intranet access for the following activities:
 - Accessing, seeking, sending, forwarding, printing, or otherwise disseminating to unauthorized persons information deemed confidential by the District.
 - Making offensive or harassing statements based on race, color, religion, national origin, ancestry, disability, age, or sex.
 - Sending or forwarding messages containing defamatory, obscene, offensive, or harassing statements. An employee should notify a supervisor and/or the Superintendent or designee immediately upon receiving such a message. This type of message should not be forwarded.
 - Attempting to access or visit sites featuring pornography, terrorism, espionage, theft, or drugs.
 - Gambling or engaging in any other criminal activity in violation of local, state, or federal law.
 - Spending excessive time using personal email accounts and social networking sites during District time, for non-educational purposes.
 - Engaging in unethical activities or content.
 - Participating in activities, including the preparation or dissemination of content, which could damage the District’s professional image, reputation and/or financial stability.
 - Permitting or granting use of an email or system account, including my own, to another employee or persons outside the District. Permitting another person to use an account or password, whose access has been denied or terminated.
 - Using another employee’s password or impersonating another person while communicating or accessing the Network or Internet without the employee’s consent.
 - Introducing a virus, harmful component, corrupted data or the malicious tampering.
 - Vandalism - Vandalism is defined as any malicious attempt to harm or destroy data of another user including any other public or private provider connected to the system. This

includes, but is not limited to, the uploading or creation of malware of any kind. Any vandalism may result in the loss of computer services, disciplinary action, and legal referral.

4. Network Etiquette and Privacy - Users of the District network are expected to abide by the generally accepted rules of network etiquette.
5. Services - The District makes no warranties of any kind, whether expressed or implied, for electronic services provided. District is not responsible for any damages suffered while on this system. Potential damages may include, but are not limited to, loss of data, non-deliveries, deliveries to unintended recipients, or service interruptions. Use of any information obtained via the information system is at the risk of the user. The District specifically denies any responsibility for the accuracy of information obtained through these services.
6. Security - Security is a high priority. Any employee identifying a security problem should notify the school administrator immediately. Never demonstrate the problem to other users. Never use another individual's account without written permission from that person. All use of the system must be under the user's assigned account. Any user identified as a security risk will be denied access to the information system.
7. Updating - The information service may occasionally require new registration and updated account information from the employee to continue the service. Employees must notify the information system of any changes in account information.
8. Social Media - When participating in social media activities, even off duty and off premises, such activities must not violate any LCBOE policies or otherwise interfere with the employee's or co-workers' job performance. All policies that govern employee behavior, ethics, performance and professionalism apply to social media, just as it would anywhere else. The Board expects all employees to exercise professionalism and good judgment in social media activities. Furthermore, social media activities must comply with all applicable laws including, but not limited to, anti-discrimination, anti-harassment, copyright, trademark, defamation, privacy, securities, and any other applicable laws and regulations.

Employees using the District's technology agree to abide by the provisions and conditions of this internet usage agreement. Employees are responsible for instructing and supervising students in their classes on acceptable use of the network and proper network etiquette.

Print name _____

Employee signature _____

Date _____