ACCEPTABLE USE POLICY, TECHNOLOGY AND INTERNET

Employees and other Non-Students

I. Introduction

This policy is applicable to all employees of Lincoln County Schools and other non-students who may obtain access to the Internet through Lincoln County Schools equipment. This policy is intended to augment and supplement State Board of Education Policy 2460, Use of the Internet by Students and Educators. This policy is in compliance with Children's Internet Protection Act (CIPA) and Children's On-line Privacy Protection Act (COPPA).

The Internet provides a source of information that can benefit every function of the District. It also improves service to students. Therefore, it is the policy of the District that employees whose job functions require or justify use of the Internet be provided access. The Administration will approve Internet access based on need and if one or more components of the Internet will be available (electronic mail (e-mail), World Wide Web (Web), newsgroups, listservs, etc.). All employees accessing the Internet-whether performing services for the District or for personal use-on District equipment, should become proficient in its capabilities, practice proper network etiquette, and agree to the conditions and requirements of this policy.

The District has a responsibility to help make the Internet a safe, secure, and productive tool for its employees and its students.

II. Policy Overview

This Acceptable Use Policy is designed to help our employees understand the District's requirements and expectations for the use of, as applicable, the Internet and all its components, the telephone system (including voice mail), facsimile machines, scanning devices, and photocopiers (collectively, Internet and technology equipment). Personal use is allowed under certain circumstances provided it in no way interferes with the intended uses of the District's resources, Internet, and technology equipment or incurs unnecessary costs to the District without prior authorization. All personal use must also be in accordance with the restrictions and requirements established in this policy.

The Internet is a tool. Access is for school-related purposes. You are required to conduct yourself appropriately on the Internet. Proper use requires that you respect all copyrights, software licensing rules, property rights, and the privacy of others, just as you would in your day-to-day job responsibilities. You must also remain security conscious and ensure that any files you receive electronically are scanned for virus contamination.

Unnecessary or unauthorized Internet usage causes network congestion. It slows other users' access, reduces effective work time, consumes supplies, and ties up printers and other shared resources. Unlawful Internet usage may expose the District to legal liabilities.

ACCEPTABLE USE POLICY, TECHNOLOGY AND INTERNET

Employees and other Non-Students

All District Internet users must agree to the following statement and positively affirm the statement with a signature. The statement will be filed with your personnel records.

"I fully understand the terms of this policy and agree to abide by them. I realize that the District may incorporate monitoring software and may record the Internet address of any site I visit. The District may keep a record of any network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive will be recorded and stored in an archive file. These archives may be accessed by law enforcement agencies when required legal processes are executed. I know that any violation of this policy could lead to dismissal or applicable criminal prosecution."

III. Policy Provisions

1. The District may have in place and use, at any time, the software and systems to monitor and record all Internet activities. These systems are capable of recording (by user) each World Wide Web site visited, chat, newsgroup, or e-mail message and each file transferred into and out of our internal networks. The District reserves the right to do so at any time. No user should have any expectation of privacy as to Internet usage.

2. The District reserves the right to inspect any and all files stored on District-owned hardware and on any personal media brought on District premises by employees to ensure compliance with this policy.

3. The purposeful display of any kind of sexually explicit or discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, or disability) image or document on any District computer or other device is a violation of this policy. In addition, none of these files may be archived, stored, distributed, edited, or recorded using District resources.

4. The District may use approved software to identify inappropriate or sexually explicit Internet sites. These sites may be blocked from access based on some specific or general criteria. If you feel your access is justified, exceptions must be approved through your supervisor and coordinated with the system administrator. If you find yourself connected incidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any filtering program, unless an exception has been justified and granted.

5. Inappropriate uses of the District's equipment, hardware, software, and Internet connectivity include:

a. Uploading, downloading, or otherwise knowingly accessing or transmitting in any fashion:

i. abusive, degrading, demeaning, derogatory, harassing or defamatory materials, information, or communications. Emphasis is added as it pertains to race, color, religion, national origin, gender, or disability.

ii. pornographic, obscene, sexually explicit, indecent, or vulgar materials, information, or communications.

iii. any confidential records of the District without adequate authority to do so. Employees must know what is and is not acceptable based on their position and function within the District.

iv. any materials or programs, including access and registration codes, which are in violation of copyright protections.

v. chain letters, distasteful jokes, gambling of any nature.

vi. use Internet or technology equipment for personal or commercial advertisements, solicitations, or promotions.

vii. any virus, worm, Trojan horse, or trap-door program code.

viii. any attempt to disable or overload any computer system or to circumvent any system intended to protect the privacy or security of another user.

b. Vandalizing, damaging, disabling, or gaining access to unauthorized computer files or data. 18 U.S.C. §1030 and W. Va. Code §61-3C-1, et seq., prohibits unauthorized individuals from accessing a computer or its data and from damaging either. This can result in a fine or imprisonment.

c. Impersonating another user, anonymity, and pseudonyms for sending e-mail or otherwise transmitting anything anonymously or under an alias unless authorized.

d. Engaging in any other activity restricted by local, state, federal, or international laws. Use of any District's resources for unlawful activity will be grounds for dismissal. The District will cooperate with any legitimate law enforcement activity.

e. Any disclosure of confidential student information protected by the Family and Educational Records Privacy Act and West Virginia Board of Education Policy.

6. Any files downloaded via the Internet or transmitted onto a District's computer or other device becomes the property of the District. Any such files may be used only in ways that are consistent with applicable licenses or copyrights.

7. Subscribed services, whether free or on a cost basis (i.e., newsgroups, listservs, etc.), and participation in chat sessions will require prior approval. A list may be published from time to time of the services that are automatically approved and for which no separate authorization is needed. When participating in any newsgroup or chat session or when sending e-mail, it is inappropriate to reveal confidential information.

8. All outgoing e-mail and postings to newsgroups, listservs, etc., must be reviewed just as though it were traditional correspondence. Improper spelling and grammar reflect poorly on the professional image of the District and its employees.

9. Use of the Internet for extended periods of time, such as file downloads longer than 30 minutes each, video and audio streaming, and use of push technologies such as PointCast, Internet Channels, or other recurring, regularly-scheduled downloads, will be permitted on a case-by-case basis by the employee's supervisor. These activities should be completed during non-peak periods if at all possible.

10. The employee should ensure that the virus protection program installed on his or her computer is running at all times except instances when approved software is being installed and only if that will interfere with the installation. Any program or file that is downloaded must be scanned for viruses before it is executed or accessed.

11. Any employee who attempts to disable or circumvent any District security program or device will be in violation of this policy and subject to disciplinary action.

12. User identifications and passwords help maintain individual accountability for computer usage. These are meant to be confidential. District policy prohibits the sharing of user identifications or passwords for use of any District computer or other device.

13. Computers at work are for District use. However, when certain criteria are met, employees are permitted to engage in the following activities:

a. During work hours, employees may access job-related information to perform specific job requirements.

b. During work hours, employees may participate in newsgroups, chat sessions, and e-mail discussion groups (listservs), provided these are job performance-related.

c. During duty-free periods, employees may retrieve non-job related text and graphics to develop or enhance Internet related skills. Adherence with this policy, and in particular, Sections III. 5 B 11, is required. This access is allowed to enhance the employee's skill set and should improve the accomplishment of job-related work assignments.

14. Employees shall abide by the requirements set forth in State Board of Education Policy 2460, Use of the Internet by Students and Educators, Children's Internet Protection Act (CIPA)and Children's On-line Privacy Protection Act (COPPA).

15. Employees are responsible for immediately reporting violations of this policy to the immediate supervisor.

IV. Audit

Internal audits will be completed periodically. The scope of the audit will include a review of users' logs as generated by any monitoring software approved by the District. Downloaded and archived documents will be periodically scanned for keywords and graphics that are not in compliance with the restrictions set forth in this policy. Hard drives will be inspected for unlicensed software. Violations will be reported to the employee's immediate supervisor.

V. Record Retention

All incoming e-mail will be retained for not less than 90 days. If it involves a dispute of any kind under investigation, retention will be indefinite.

Employee discretion should be used with respect to printing messages for retention with other documents for convenience.

VI. Enforcement

Violations of this policy may result in disciplinary actions. Depending on the severity or frequency of the violations, this could include:

- counseling statements for policy violations.
- a written letter of reprimand.
- a suspension/termination of Internet or PC use privileges.
- a suspension or termination of employment.
- the payment of any fees for unauthorized services.
- the payment of any fines or back license fees associated with the installation of unlicensed software, including reimbursement of the District for any settlement that may be negotiated in connection with copyright violations that are attributed to employee misconduct.
- personal liability under applicable local, state, federal, or international laws.

Employees retain this portion for your records

ACCEPTABLE USE POLICY, TECHNOLOGY AND INTERNET

Employees and other Non-Students

Acceptable Use Policy, Technology and Internet (Employees and other non-students)

Statement of Understanding

I fully understand the terms of the above Acceptable Use Policy and agree to abide by them.

I realize that the District may incorporate monitoring software and may record the Internet address of any site I visit.

The District may keep a record of any network activity in which I transmit or receive any kind of file.

I acknowledge that any message I send or receive will be recorded and stored in an archive file. These archives may be accessed by law enforcement agencies when required legal processes are executed.

I know that any violation of this policy could lead to dismissal or applicable criminal prosecution.

I have read the aforesaid consent and waiver for use of telecommunications in the schools.

I understand that this access is for educational purposes only and restricted to school use only.

Employee Name _____ Date _____

Employee ID Number _____