Acceptable Use / Internet Safety Policy

All use of the LEE COUNTY School Division's computer system shall be consistent with the School Board's goal of promoting educational excellence by facilitating resource sharing, innovation and communication. Over the past several years, Lee County School System has made vast improvements and investments in technology. There are computers with network access in classrooms, media centers, and technology labs. This access is provided because of the wealth of educational resources available on the Internet. This technology will also enable us to fulfill the mandates of Virginia's Web-based SOL Technology Initiative.

The purpose of our Acceptable Use / Internet Safety Policy is to describe the appropriate uses of the Lee County School Board's computers, networks, Internet access, and other technology resources. It specifically addresses the issues described in the federal Children's Internet Protection Act (CIPA):

- access by minors to inappropriate matter on the Internet and World Wide Web;
- the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
- unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
- unauthorized disclosure, use, and dissemination of personal information regarding minors; and
- measures designed to restrict minors' access to materials harmful to minors.

Computer System Use-Terms and Conditions:

1. Acceptable Use. Access to the Division's computer system shall be (1) for the purposes of education or research and be consistent with the educational objectives of the Division or   (2) for legitimate school business.

2. Privilege. The use of the Division's computer system is a privilege, not a right.

3. Unacceptable Use. Each user is responsible for his or her actions on the computer system. Prohibited conduct includes:

    - using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any federal, state or local law.

    - sending, receiving, viewing or downloading illegal material via the computer system.

    - unauthorized downloading of software .

    - downloading copyrighted material for unauthorized use.

    - using the computer system for private financial or commercial gain.

- wastefully using resources, such as file space.

- gaining unauthorized access to resources or entities.

- posting material authorized or created by another without his or her consent.

- using the computer system for commercial or private advertising.

- submitting, posting, publishing or displaying any obscene, profane, threatening, illegal or other inappropriate material.

- using the computer system while access privileges are suspended or revoked.

- vandalizing the computer system, including destroying data by creating or spreading viruses or by other means.

4. Network Etiquette. Each user is expected to abide by generally accepted rules of etiquette, including the following:

- Be polite.

- Users shall not forge, intercept or interfere with electronic mail messages.

- Use appropriate language. The use of obscene, lewd, profane, threatening or disrespectful language is prohibited.

- Users shall not post personal contact information about themselves or others.

- Users shall respect the computer system's resource limits.

- Users shall not post chain letters or download large files.

- Users shall not use the computer system to disrupt others.

- Users shall not read, modify or delete data owned by others.

5. Liability. The School Board makes no warranties for the computer system it provides. The School Board shall not be responsible for any damages to the user from use of the computer system, including loss of data, non-delivery or missed delivery of information, or service interruptions. The School Division denies any responsibility for the accuracy or quality of information obtained through the computer system. The user agrees to indemnify the School Board for any losses, costs or damages incurred by the School Board relating to or arising out of any violation of these procedures.

6. Security. Computer system security is a high priority for the school division. If any user identifies a security problem, the user shall notify the building principal or system administrator immediately. All users shall keep their passwords confidential and shall follow computer virus protection procedures.

7.   Vandalism. Intentional destruction of any part of the computer system through creating or downloading computer viruses or by any other means is prohibited.

8.   Charges. The School Division assumes no responsibility for any unauthorized charges or fees as a result of using the computer system, including telephone or long-distance charges.

9.   Electronic Mail.   The School Division's electronic mail system is owned and controlled by the School Division. The School Division may provide electronic mail to aid students and staff in fulfilling their duties and as an education tool. Electronic mail is not private. Student's electronic mail will be monitored. The electronic mail of staff may be monitored and accessed by the School Division. Unauthorized access to an electronic mail account by any student or employee is prohibited. Users shall be held personally liable for the content of any electronic message they create. Downloading any file attached to an electronic message is prohibited unless the user is certain of that message's authenticity and the nature of the file.

10.   Enforcement. Software will be installed on the division's computers having Internet access to filter or block internet access through such computers to child pornography and obscenity. The online activities of minors may also be monitored manually. Any violation of these regulations shall result in loss of computer system privileges and may also result in appropriate disciplinary action, as determined by School Board policy, or legal action.

Internet Filtering and Monitoring

The Lee County School Board's computers, networks, and technology resources are for instructional and administrative usage. Specific approved usages include research, taking classes on the Internet, and use in academic classes. The Internet provides a wealth of material that supports our educational mission.

The Internet also contains pornographic material, Web sites run by hate groups, and information on how to commit crimes. To prevent this information from entering our schools, we use an Internet filtering program. This program has a database of pornographic and other objectionable Web sites. We have configured the filtering program to block access to these Web sites.

Although the filtering program's database is updated several times a week, there is always the possibility that a new pornographic or hate site will appear that has not been picked up by the program. For that reason, our teachers, librarians, and other staff members also monitor and supervise students' Internet access. Records of Internet access are also stored in computer log files, which we monitor periodically. These efforts help students learn how to use the Internet responsibly and avoid unsuitable sites. **Students who deliberately attempt to access pornographic and other blocked sites are subject to disciplinary procedures. This includes using anonymous proxies and anonymizers to bypass the filtering system.**

Although our filtering software and monitoring efforts are designed to make the Internet an educational and safe experience, they cannot completely eliminate the risk that students will be able to access inappropriate material. Therefore, parents may choose to opt their children out of accessing the Internet at school. There is a form provided at the end of this policy for this purpose.

Penalties for Violations of the Internet Safety/Technology Usage Policy
Violations of the Internet Safety/Technology Usage Policy will be handled by school staff in the same fashion as other disciplinary matters.

Preventing Unauthorized Disclosure, Use, and Dissemination of Personal Information

Federal and state laws govern the disclosure, use, and dissemination of personal information regarding students and school board employees. Because much of that information is contained in computer databases, School Board employees must take precautions to ensure the integrity of that data.

- Staff members with access to student and staff information should not share their passwords with anyone else, including other employees.
- Staff members should never give their passwords to anyone over the phone. (Computer hackers sometimes gain access to computer networks by calling a secretary, pretending to be a technical support person, and telling the secretary that they need her password to fix a problem.)
- Staff members should not leave their computers unattended when they are logged in with access to student or staff information records.
- Staff members should ensure that backups of student and personnel information are protected from theft or tampering.
- Staff members should review any requests for student or personnel information from outside sources with their principal or a designated person at the Central Office before releasing that information.
- Students should not use school computers to complete any Internet-based forms that request the student's name, phone number, address, or other personal information, unless the organization posting the form is affiliated with the Lee County School Board, such as the A. Linwood Holton Governor's School.
- Schools should not publish any information on Web sites that would enable a visitor to the site to match a student's picture with the student's name. Schools may publish honor roll lists and other information similar to what we send to area newspapers, but should not publish an accompanying photograph that would enable a site visitor to match a student's name with his/her picture. Schools should never publish student addresses, phone numbers, or parent/guardian names on the World Wide Web.

Installing Software or Modifying Computer Systems

Students are not allowed to install or remove software on any computers belonging to the Lee County School Board, unless they have the express permission of the school principal or the principal's designated staff member. This means that students may not bring games from home and install them on School Board computers, or download software from the Internet and install it on School Board computers.

Students are not allowed to modify the setup of computer systems belonging to the School Board. This means that students should not change any settings on a School Board computer, any Internet browser settings, or the names of any files on a School Board computer, except for files created by the student for academic use.

There are several reasons we restrict students from installing software or otherwise modifying computer systems:

1. Some computer games have violent or sexual themes that are not appropriate for school.

2. Some software is designed to enable users to "hack" into computer systems that they are not authorized to access.

3. Any software installation carries with it the possibility of making the computer malfunction. This is particularly true with some games that change the computer's system settings.

4. Software downloaded from the Internet may be infected with a virus or a Trojan horse. (A Trojan horse is software that permits an intruder to secretly gain access to a computer.)

5. Many different people use School Board computers. If we allow students to change the names of program icons, other users may not be able to find the programs they need.

6. Modifying the system setup could cause a computer to malfunction or bypass the Internet filtering system.

Staff members should also consult with the School Board's Technology Director before installing software on school computers, to ensure that the software is properly licensed and compatible with the school's computers and networks.

E-Mail, Instant Messaging, Chat Rooms, and Social Networking Sites

Unauthorized e-mail, instant messaging, Internet chat rooms, and social networking sites such as MySpace and FaceBook consume network bandwidth that is needed for instructional and administrative use. They also expose students to harassing or threatening messages. Even friendly usage of these applications can distract students from school work, in the same manner as cellular telephones and pagers, which are also prohibited. Therefore, the Lee County School Board will not allow students to use School Board computers to access e-mail, instant messaging programs, Internet chat rooms, or social networking sites unless those applications are required for a class the student is taking. The decision as to whether these applications are required for a specific academic purpose rests with the school principal.

As required by Virginia law, Lee County schools also incorporate Internet safety instruction into their curriculum. The goal of this instruction is to make students aware of the risks of certain kinds of online behavior, such as posting personal or financial information online and violating copyright legislation by illegally sharing media files.

Parents should also be aware that people can use e-mail, instant messaging software, chat rooms, and social networking sites to threaten, harass, or entice their children. Some pornographic Web sites also solicit visitors through e-mail and instant messaging software, such as ICQ and AOL Instant Messenger. It can be extremely difficult to trace the source of these inappropriate messages. If you decide to allow your children to access e-mail, instant messaging software, or social networking sites at home, we suggest that you encourage your children to use "handles," or pseudonyms for their online accounts. Your child should also not provide an address, phone number, or other personal information to anyone they meet through e-mail, instant messaging, or social networking.

If your child does receive a threatening or harassing e-mail or message, DO NOT ERASE the message. If you keep the original message, law enforcement authorities may be able to trace the message to its sender, even if the sender used a forged e-mail address.

Annual Evaluation of This Policy

The School System's Director of Technology shall be responsible for collecting suggestions for improvements to this policy throughout the school year from teachers and other school board employees, students, parents, and community members. In addition, the Internet Safety/Technology Usage Policy and the Internet Safety Instruction curriculum will be a topic of discussion at regularly scheduled administrative staff meetings throughout the year. The Director of Technology will compile and present revisions to this policy to the Division Superintendent once a year. The Division Superintendent will present the revisions to the School Board for consideration prior to the beginning of each new school year.

Suggested guidelines for teachers, students, administrators, parents/guardians, and community members:

1. Discuss internet use with your students/children and clarify what they should and should not do online.
2. Make your expectations about Internet use clear to your students/children.
3. Advise your students/children never to reveal their name, address, phone number or school name online without your permission, including in chat rooms and in postings to discussion boards, bulletin boards or other online forums. The Internet is a public place and protecting personal privacy is essential.
4. Advise your students/children never to upload a picture of themselves to the Internet or send it as an e-mail attachment to anyone they do not know.
5. Periodically monitor your students'/children's use of the computer- what they are doing at a particular moment as well as their Internet history.
6. Use a filtered Internet Service Provider (ISP).
7. Check for wireless access points in your neighborhood. Encourage your community members to password protect their wireless networks because laptops can access wireless networks in the community.
8. Encourage your students/children to share their knowledge of the Internet and online learning experiences with you, and to come to you with any concerns.
9. Ask your students/children to show you their favorite websites.
10. Ask your students/children to tell you about the exciting learning they have experienced online as part of their classroom or library activities.
11. Encourage your students/children to come to you if they feel uncomfortable about information they see on online or receive via e-mail.
12. If someone sends a message or image to your students/children that are inappropriate or indecent, report it to you. You may also report the incident to the Virginia State Police Cybercrimes Unit at 804-553-3413 or to the CyberTipline of the National Center for Missing and Exploited Children by calling 1-800-843-5678 or submitting an online report at www.missingkids.com/cybertip.

Dear Parent/Guardian:

The LEE COUNTY SCHOOL BOARD offers your student the use of electronic communications through the LEE COUNTY SCHOOL DIVISION's computer system. Your student will be able to communicate with other schools, colleges, organizations, and individuals around the world through the internet and other electronic information systems/networks.

Part of the school division's responsibility in preparing students for the 21st century is to provide them access to the tools they will be using as adults. The internet will likely be one of these tools. Through the division's computer system your student will have access to databases, libraries, and computer services from all over the world. We accept the responsibility of teaching your student about his/her role as a "network" citizen and the code of ethics involved with this new community.

With this educational opportunity also comes responsibility on the part of your student. It is important that you and your student read the enclosed division policy, administrative regulation and agreement form, and discuss these requirements. The division takes precautions to prevent access to inappropriate material. However, it is impossible to control access to all material and a user may access inappropriate material.

In order for your student to take advantage of this educational opportunity, your authorization is needed. Attached to this letter are the Acceptable Computer System Use Policy and Regulation (GAB/IIBEA) and the Acceptable Computer System Use Agreement which both you and your student must sign before your child may use the computer system. Please review these materials carefully with your student before the required agreement.

Sincerely,

Acceptable Use / Internet Safety Policy

Each student must sign this Agreement as a condition for using the school Division's computer system. Each student and his/her parent/guardian must sign this Agreement before being granted use of the school division's computer system. **Read this Agreement carefully before signing.**

If you have any questions about this policy or regulation, contact your supervisor or your student's principal.

I understand and agree to abide by the school division's Acceptable Computer System Use Policy and Regulation. I understand that the school division may access and monitor my use of the computer system, including my use of the internet, email, and downloaded material, without prior notice to me. I further understand that should I violate the Acceptable Use Policy or Regulation, my computer system privileges may be revoked and disciplinary action and/or legal action may be taken against me.

Student Signature: _____
Date: _____

I have read this Agreement and Policy and Regulation GAB/IIBEA. I understand that access to the computer system is intended for educational purposes and the LEE COUNTY SCHOOL DIVISION has taken precautions to eliminate inappropriate material. I also recognize, however, that it is impossible for the school division to restrict access to all inappropriate material and I will not hold the school division responsible for information acquired on the computer system. I have discussed the terms of this agreement, policy, and regulation with my student.

I grant permission for my student to use the computer system and for the school division to issue an account for my student.

Parent/Guardian Signature: _____
Date: _____

Parent/Guardian Name: _____
                              (Please Print)

Each employee, substitute, student teacher, parents/guardians, or community members must sign this Agreement as a condition for using the school Division's computer system.

I understand and agree to abide by the school division's Acceptable Computer System Use Policy and Regulation. I understand that the school division may access and monitor my use of the computer system, including my use of the internet, email, and downloaded material, without prior notice to me. I further understand that should I violate the Acceptable Use Policy or Regulation, my computer system privileges may be revoked and disciplinary action and/or legal action may be taken against me.

Signature: _____

Date: _____

Read this Agreement carefully before signing.

Request to Opt Student Out of School Internet Access

As the parent or legal guardian of _____, a minor, I wish to opt _____ out of accessing the Internet at school. I understand that in doing so, I may prevent my child from accessing the Internet-based instructional materials and activities that will be available to his classmates. The Lee County School System will provide alternative activities for children whose parents do not wish them to access the Internet; however, the Lee County School Board cannot ensure that these activities will provide the same richness and depth of experience that access to the Internet can provide. Please note that this opt-out form does not opt your child out of Lee County's online SOL assessment program. Online SOL assessments are delivered across the Internet through special software that only allows the student to access the SOL test questions.

Parent/Guardian Signature: _____
Date: _____

Parent/Guardian Name: _____
                                        (Please Print)