

## **CHAPTER 8.00 – MAINTENANCE SERVICES**

### **8.21 – ELECTRONIC SYSTEMS RESPONSIBLE USE**

#### **POLICY:**

The School Board of Levy County provides a variety of electronic communication systems for educational purposes. The electronic communications system is defined as the District's network (including the wireless network), servers, computer workstations, mobile technologies, peripherals, applications, databases, online resources, internet access, email, and other technology designated for use by students and employees, including all new technologies as they become available. Including any access to the School Board of Levy County electronics system while on or near school property, in school vehicles and at school sponsored activities, and consists of the appropriate use of district technology resources via off-campus remote access. Use of any other network or computing resources on school property or at school events must be consistent with the rules and procedures outlined in this policy.

#### **1. Telephone Service**

- a. In order to promote efficiency and economy, the Superintendent or designee shall develop a uniform system for implementing effective telephone service systems. School personnel shall be informed of this system.
- b. Employees are generally not permitted to use the District System to conduct personal business or for other personal purposes. However, limited personal use of the system is permitted, but only to the extent it does not conflict with the user's employment duties and responsibilities. Employees may use the telephone system to make calls on their breaks. Such calls should be brief and infrequent so as not to interfere with the official use of the system.
- c. Logs shall be maintained of long distance calls by work location. Logs shall be in a uniform format. Telephone service billings and long distance logs shall be subject to periodic review and audit. No person shall charge personal calls to the School Board.

#### **2. Internet Use**

- a. The District is required to comply with state and federal data privacy laws. Employees are required to safeguard employee and student data they have access to in the course of performing their duties. They are required to safeguard their network/system credentials to protect student and employee data from hacks and unauthorized access. The District will provide employees with training in sound email and Internet security practices.

## **CHAPTER 8.00 – MAINTENANCE SERVICES**

- b. As required by the Children Internet Protection Act (CIPA), the School District educates staff and students regarding appropriate online behavior to ensure internet safety, including use of email and internet resources. An internet filter is maintained by the school district for school use on all district network connections. Filtering not only restricts access to unacceptable sites, but also restricts access to inappropriate content such as those that are illegal, harmful, or contain potentially offensive information. The School Board of Levy County cannot guarantee that access to all inappropriate sites will be blocked. Log files are maintained on each device with a detailed history of all sites accessed. It is the responsibility of the user to appropriately use the device, network, and the internet.
- c. Each student, parent as defined by Florida Statutes, visitor and employee of the District will be required to sign an agreement for network responsibility wherein they are acknowledging their obligation to comply with the terms and conditions outlined in this policy.
- d. Appropriate Use
  - 1. Students, staff and visitors may only open, view, modify, and delete their computer files.
  - 2. Internet use at school must be directly related to school assignments and projects.
  - 3. Students, staff and visitors may be assigned individual network accounts and email accounts and must use only those accounts and passwords that they have been granted permission by the district to use. All account activity should be for educational purposes only.
  - 4. Students, staff and visitors must immediately report threatening messages or discomforting Internet files/sites to a teacher.
  - 5. Students must at all times use the district's electronic communications system, including email when necessary, wireless network access, and Web 2.0 tools/ resources to communicate only in ways that are kind and respectful. (Web 2.0 tools allow users to interact and collaborate in virtual communities, where users are active creators of content i.e. wikis, video sharing sites, cloud service).

## **CHAPTER 8.00 – MAINTENANCE SERVICES**

6. Students, staff and visitors are responsible at all times for their use of the district's electronic communications system and must assume personal responsibility to behave ethically and responsibly, even when technology provides them the freedom to do otherwise.
- e. Inappropriate Use
1. Use of other Internet Service Providers (ISPs), wireless access points (WAPs) and wireless hotspots not provided by the School District are prohibited on the School District network.
  2. Using the district's electronic communications system for illegal purposes including, but not limited to, cyberbullying, gambling, pornography, and computer hacking.
  3. Using a Virtual Private Network (VPN) program to bypass the School District filtering and or monitoring systems.
  4. Disabling or attempting to disable any system monitoring or filtering or security measures.
  5. Sharing user names and passwords with others; and or borrowing someone else's username, password, or account access.
  6. Purposefully opening, viewing, using or deleting files belonging to another system user without permission.
  7. Electronically posting personal information about one's self or others (i.e., addresses, phone numbers, and pictures).
  8. Downloading or plagiarizing copyrighted information without permission from the copyright holder.
  9. Intentionally introducing a virus or other malicious programs onto the district's system.
  10. Electronically posting messages or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
  11. Gaining unauthorized access to restricted information or network resources.
  12. Using a computer or the network for illegal purposes.
  13. Violating student or staff's rights to privacy.
  14. Using profanity, obscenity, or other language which may be offensive to another user.

## **CHAPTER 8.00 – MAINTENANCE SERVICES**

15. Sending or receiving pornographic text and/or graphics.
  16. Sexting shall be prohibited. All acts of alleged sexting shall be reported to the appropriate legal authority.
  17. Sending or receiving copyrighted materials, including computer software, without permission, or material protected by trade secrets.
  18. Using for commercial activities, product advertisement, or political lobbying.
- f. Special Note: Cyberbullying. Cyberbullying is defined as the use of any Internet-connected (electronic) device for the purpose of bullying, harassing, threatening, embarrassing or intimidating another student or school staff. Including, but not be limited to:
1. Sending abusive or offensive text messages to cell phones, computers, or Internet-connected game consoles.
  2. Posting abusive or offensive comments on someone's blog or social networking site (e.g., Facebook, Instagram, Snap Chat, etc.).
  3. Creating a social networking site or web page that masquerades as the victim's personal site and using it to embarrass him or her.
  4. Making it appear that the victim is posting malicious comments about friends to isolate him or her from friends.
  5. Displaying the victim's personally identifiable information on a site to put them at risk of contact by predators.
  6. Sending abusive comments while playing interactive games.
  7. Recording and distributing media with the intent to manipulate or embarrass others.
- g. Internet Warning. At school, students' access to and use of the network will be under staff direction and monitored as any other classroom activity. The District is not able to prevent the possibility of user access to material that is not consistent with the education mission, goals, and policies of the School Board when access is obtained outside of the school.
- h. User Guidelines.
1. Internet access is coordinated through a complex association of government agencies and regional and state networks.

## **CHAPTER 8.00 – MAINTENANCE SERVICES**

It is the District's intent that the Internet and our communications network be used in a responsible, efficient, ethical, and legal manner. The operation of the Internet relies heavily on the proper conduct of the users who must adhere to strict guidelines. If a district user violates any of these provisions, their account will be restricted. Serious violations may result in school disciplinary action or legal action. The signature(s) on the acceptable use agreement indicate that the user(s) have read the terms and conditions carefully and understand their significance.

2. Acceptable Use. The use of your account must be in support of education and research that is consistent with the educational goals and policies of the District. Users are encouraged to develop uses which meet their individual needs and that take advantage of the network's function; electronic mail, conferences, bulletin boards, data bases, and access to the Internet. Use of any other network or computing resources must be consistent with the rules appropriate to that network.
  3. Privileges. The use of Internet is a privilege. Inappropriate use will result in the restriction of that privilege. Each individual who accepts an account will receive information pertaining to the proper use of the network. School and district administrators will decide what is "inappropriate use". Their decision is final. An account may be closed by the district at any time deemed necessary or by recommendation of the administration, faculty, or staff. The person in whose name an account is issued is responsible at all times for its proper use.
  4. "Netiquette". You are expected to abide by the generally accepted rules of network etiquette. Be polite. Do not use vulgar or obscene language. Do not reveal your address or phone number, or those of others. Please remember that electronic mail is not guaranteed to be private. Do not disrupt the network, the data, or other users.
- i. Warranties: The District makes no warranties of any kind, whether expressed or implied, for the service it is providing.

The District will not be responsible for any damage you suffer including loss of data. The District will not be responsible for the accuracy or quality of information obtained through this Internet connection.

## **CHAPTER 8.00 – MAINTENANCE SERVICES**

- j. Security. Security is a high priority. If you identify a security problem, you must notify a system administrator immediately. Do not show or identify the problem to others. Do not use another individual's account. Attempts to log on as another user will result in cancellation of your privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access.
- k. Vandalism. Vandalism will result in cancellation of your privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks. This includes the creation of or the unloading of computer viruses on to the Internet or host site. Deliberate attempts to degrade or disrupt system performance will be viewed as criminal activity under applicable state and federal law.
- l. E-mail Etiquette. Helpful to your e-mail success are:
  - 1. Preparing text files for uploading before logging on;
  - 2. Making "subject" heading as descriptive as possible.  
CHAPTER 8.00 – AUXILIARY SERVICES ©NEFEC Page 6 of 8 NEFEC 8.33\*+ New: 2/11/22
  - 3. Beginning messages with a salutation; restating the question or issue being addressed in a response;
  - 4. Choosing words carefully to avoid misunderstandings; text does not permit the verbal or expression clues which are usually necessary when statements are intended to be funny or sarcastic;
  - 5. Ending messages with your name and your e-mail address to assist getting feedback or clarifications;
  - 6. Logging off before editing and printing downloaded files; and
  - 7. Deleting e-mail files as soon as possible as appropriate under public records law.
- m. Staff are responsible for teaching proper techniques and standards for participation, guiding student access to appropriate sections of the network, and or assuring students understand that if they misuse the network they will lose their access privileges. Conference moderators are responsible for monitoring the context and tone of posted messages and or taking steps to delete offensive materials and to communicate with authors.

## **CHAPTER 8.00 – MAINTENANCE SERVICES**

- n. Contracts. Students, staff and visitors are required to enter into an "Electronics Systems Responsible Use Agreement". Employees are required to enter into an Employee Electronics Systems Responsible Use Agreement". These forms shall be approved by the School Board.
- o. Exception of Terms and Conditions. All terms and conditions stated in this document are applicable to all users of the network. These terms and conditions reflect an agreement of the parties and shall be governed and interpreted in accordance with the laws of the United States of America, the state of Florida, and the School Board.

3. Employee Electronic Systems Responsible Use Agreement School Board  
Policy # 8.33 Please print all information User's full  
Name: \_\_\_\_\_  
Home Phone: \_\_\_\_\_ Work Phone: \_\_\_\_\_  
Employee Location: \_\_\_\_\_  
Job Title: \_\_\_\_\_

### **EMPLOYEE AGREEMENT**

I have read and understand the Terms and Conditions of the Electronic Systems Responsible Use policy (School Board Policy 8.33) and the Use of Social Media policy (School Board Policy 8.33). I agree to comply with these policies and understand that violations may result in losing my access privileges. In addition, violations may result in disciplinary action including termination of employment and/or appropriate legal or criminal action being initiated against me. Employee

Signature: \_\_\_\_\_  
Date \_\_\_\_\_  
Supervisor's Signature: \_\_\_\_\_  
Date \_\_\_\_\_

4. Student/Parent Contract Student/Parent Network Responsibility Contract  
School Board Policy 8.33 Please print all information User's full  
Name: \_\_\_\_\_  
School: \_\_\_\_\_  
Grade: \_\_\_\_\_

## **CHAPTER 8.00 – MAINTENANCE SERVICES**

### **STUDENT AGREEMENT**

I understand and will abide by the Terms and Conditions of the Electronic Systems Responsible Use Policy. Violations may result in the restriction or suspension of my access privileges.

In addition, violations may result in school disciplinary action and/or appropriate legal or criminal action being initiated against me.

Student Signature: \_\_\_\_\_

Date \_\_\_\_\_

### **PARENT/VISITOR**

(Also required if student is under the age of 18)

As the parent or guardian of this student, I have read the terms and conditions of the Electronic Systems Responsible Use Policy. I understand that this access is designed solely for educational purposes and the School District has taken reasonable precautions to supervise and filter Internet usage. I also recognize it is impossible for the District to restrict access to all controversial materials and I will not hold the district responsible for information acquired or contracts made on the network. Further, I accept full responsibility for supervision of Internet usage by my child outside of the school setting. I hereby give permission to establish network privileges for my child and certify that the information contained on this form is true and correct to the best of my knowledge and belief.

Parent/Visitor Signature \_\_\_\_\_ Date \_\_\_\_\_

Parent/Visitor Name (Please print) \_\_\_\_\_

Parent/Visitor Work Phone: \_\_\_\_\_

5. Consequences for Inappropriate Use
  - a. Appropriate disciplinary or legal action in accordance with the Student Code of Conduct and applicable laws including monetary damages shall govern student discipline for student violation of this policy.
  - b. Suspension of access to the district's electronic communications system.
  - c. Revocation of the district's electronic communications system account(s); and or



## ***CHAPTER 8.00 – MAINTENANCE SERVICES***

- d. Termination of System User Account: The district may deny, revoke, or suspend specific user's access to the district's system with or without cause or notice for lack of use, violation of policy or regulations regarding acceptable network use, or as a result of disciplinary actions against the user
- e. Possible criminal charges
- f. Employee violation of this policy may result in disciplinary actions including termination of employment.

### **STATUTORY AUTHORITY:**

1001.42, F.S.

### **LAW(S) IMPLEMENTED:**

1000.21, 1001.43, F.S.

### **HISTORY:**

Adopted: 7/21/22

Revision Date(s):

Formerly: