Internet Acceptable Use

Students must adhere to and support all policies and implementing regulations issued by the Cobb County School District, including Administrative Rule IFBG-R (Technology Acceptable Use). Students who violate District/school policies, Rules o regulations governing the use of the District's technology and network resources may have their network privileges suspended or revoked and will be subject to District Administrative Rules applying to student conduct including the provisions of the appropriate District Code of Conduct (Administrative Rule JCDA-R)

Ethical use of District technology prohibits the following activities by all users:

1. Accessing, sending, creating or posting material or communication that is: Damaging; abusive; obscene, lewd, profane, offensive, indecent, sexually explicit, or pornographic; threatening or demeaning to another person; or contrary to the District's Rules on harassment and/or bullying.

2. Posting anonymous or forging electronic communications.

3. Using the network for financial gain, advertising or political lobbying to include student elections.

4. Engaging in any activity that wastes, monopolizes, or compromises the District/school's technology or other resources.

5. Illegal activity, including but not limited to copying or downloading copyrighted software, music or images, or violations of copyright laws.

6. Using the District network for downloading music or video files or any other files that are not for an educational purpose or, for students, a teacher-directed assignment.

7. Attempting to gain unauthorized access to District/school technology resources whether on or off school property.

8. Using non-educational Internet games, whether individual or multi-user.

9. Participate in any online communication that is not for educational purposes or, for students, that are not specifically assigned by a teacher.

10. Using voice over IP, internet telephony, video and/or audio communication devices without teacher supervision.

11. Using District/school technology resources to gain unauthorized access to another computer system whether on or off school property (e.g. “hacking”).

12. Attempting to or disrupting District/school technology resources by destroying, altering, or otherwise modifying technology, including but not limited to, files, data, passwords, creating or spreading computer viruses, worms, or Trojan horses; engaging in DOS attacks; or participating in other disruptive activities.

13. Bringing on premises any disk or storage device that contains a software application or utility that could be used to alter the configuration of the operating system or network equipment, scan or probe the network, or provide access to unauthorized areas or data.

14. Attempting/threatening to damage, destroy, vandalize, or steal private/school property while using school technology resources.

15. Bypassing or attempting to circumvent network security, virus protection, network filtering, or policies.

16. Using or attempting to use the password or account of another person, utilizing a computer while logged on under another user’s account, or any attempt to gain unauthorized access to accounts on the network.

17. Connecting to or installing any personal technology computing device or software without prior approval of the District’s Technology Services Division. 18. Disclosing or failing to secure account password(s).

19. Exploring the configuration of the computer operating system or network, running programs not on the, or attempting to do anything not specifically authorized by District personnel or policies, Rules or regulations.

20. Leaving an unsecured workstation without logging out of the network.

21. Exploring the configuration of the computer operating system or network, running programs not approved for use, or attempting to do anything not specifically authorized by District personnel or policies, Rules or regulations

22. Leaving an unsecured workstation without logging out of the network.

23. Executing or installing software or applications not approved by the District's Technology Services Division.

24. Failing to notify appropriate District personnel of potential security incidents.

For the full text of Administrative Rule IFBG-R, visit the District website at www.cobbk12.org. Locate and click on 'Policies & Rules' under the 'About CCSD' menu option.