ACCEPTABLE USE OF THE COMPUTERS, NETWORK, INTERNET, ELECTRONIC COMMUNICATIONS AND INFORMATION SYSTEMS (CIS)

This policy describes how students and staff members may access the District's networks and defines unacceptable Internet practices, allowing for the District to track and/or monitor network traffic and to provide, restrict or revoke access privileges if usage is deemed unacceptable.

Users are prohibited from using school district CIS systems to:

1. Communicate about non-work or non-school-related communications unless the employees' use comports with this policy's definition of incidental personal use.

2. Send, receive, view, download, access or transmit material that is harmful to minors, indecent, obscene, pornographic, child pornographic, terroristic, or advocates the destruction of property.

3. **Send, receive, view, download, access or transmit inappropriate matter and material likely to be offensive or objectionable to recipients including, but not limited to,** that which may be defamatory; inaccurate; obscene, sexually explicit; lewd, hateful, harassing, discriminatory as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability; violent, vulgar, rude; inflammatory; threatening; profane; pornographic; offensive; terroristic and/or illegal.

4. **Cyber-bullying** (i.e. myspace.com; youtube.com; etc.) another individual.

5. Access or transmit gambling pools for money, including but not limited to, basketball and football, or any other betting or games of chance.

6. Participate in discussion or news groups that cover inappropriate and/or objectionable topics or materials, including those that conform to the definition of inappropriate matter in this policy.

7. **Send terroristic threats, hateful mail, harassing communications,** discriminatory remarks, and offensive, profane, or inflammatory communications.

8. **Participate in unauthorized Internet Relay Chats, instant messaging communications and Internet voice communications (online; real-time conversations) that are not for school-related purposes or required for employees to perform their job duties.**

9. Facilitate any illegal activity.

10. Communicate through e-mail for non-educational purposes or activities, unless it is for an incidental personal use as defined in this policy. The use of e-mail to mass mail non-educational or non-work related information is expressly prohibited. For example, the use of the everyone distribution list, building level distribution lists, or other e-mail distribution lists to offer personal items for sale is prohibited.

11. Engage in commercial, for-profit, or any business purposes, except where such activities are otherwise permitted or authorized under applicable district policies; conduct unauthorized fundraising or advertising on behalf of the district and non-school organizations; resell district computer resources to individuals or organizations; or use the district's name in any unauthorized manner that would reflect negatively on the school district, its employees, or students. Commercial purpose is defined as offering or providing goods or services or purchasing goods or services for personal use. School district acquisition policies will be following for district purchase of goods or supplies through the school district system.

12. Political lobbying.

13. **Install, distribute, reproduce or use copyrighted software on district computers, or copy district software to unauthorized computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright, as described in this policy.**

14. Install computer hardware, peripheral devices, network hardware or system hardware. The authority to install hardware or devices on district computers is restricted to the Superintendent or the designated official.

15. Encrypt messages using encryption software that is not authorized by the district from any access point on district equipment or district property. Employees and students must use district-approved encryption to protect the confidentiality of sensitive or critical information in the district's approved manner.

16. Access, interfere, possess, or distribute confidential or private information without permission of the district's administration. An example includes accessing other students' accounts to obtain their grades.

17. Violate the privacy or security of electronic information.

18. Use the systems to send any district information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the district's business, or educational interest.

19. Send unsolicited commercial electronic mail messages, also known as spam.

20. Post personal or professional web pages without administrative approval.

21. **Post anonymous messages.**

*Please refer to **Policy #815** online at **www.allentownsd.org** and/or a paper version at your child's school.*