EMPLOYEE COMPUTER AND INTERNET USE RULES

The intent of these board-level rules is to provide employees with general requirements for utilizing the school unit's computers, networks and Internet services. The board rules may be supplemented by more specific administrative procedures and rules governing day-to-day management and operation of the computer system.

These rules provide general guidelines and examples of prohibited uses for illustrative purposes but do not attempt to state all required or prohibited activities or use is acceptable should seek further guidance from the system administrator.

Failure to comply with board policy GCSA, these rules and/or other established procedures or rules governing computer use may result in disciplinary action, up to and including discharge. Illegal uses of the school unit's computers will also result in referral to law enforcement authorities.

A. Access to School Computers, Networks and Internet Services

The level of access that employees have to school unit computers, networks and Internet services is based upon specific employee job requirements and needs.

B. Acceptable Use

Employee access to the school unit's computers, networks and Internet services is provided for administrative, educational, communication and research purposes consistent with the school unit's educational mission, curriculum and instructional goals. General rules and exceptions for professional behavior and communication apply to use of the school unit's computers, networks and Internet services.

Employees are to utilize the school unit's computers, networks and Internet services for school-related purposes and performance of job duties. Incidental personal use of computers is permitted as long as such use does not interfere with the employee's job duties and performance, with system operation or other system users. "Incidental personal use" is defined as use by an individual employee for occasional personal communications. Employees are reminded that such personal use must comply with this policy and all other applicable policies, procedures and rules.

C. Prohibited Use

The employee is responsible for his/her actions and activities involving school unit computers, networks and Internet services and for his/her computer files, passwords and accounts. General examples of unacceptable uses that are expressly prohibited include but are not limited to:

1. Any use that is illegal or in violation of other board policies, including harassing, discriminatory or threatening communications and behavior, violations of copyright laws, etc.;

2. Any use involving materials that are obscene, pornographic, sexually explicit or sexually suggestive;

3. Any inappropriate communications with students or minors;

4. Any use for private financial gain, or commercial, advertising or solicitation purposes;

5. Any use as a forum for communicating by e-mail or any other medium with other school users or outside parties to solicit, proselytize, advocate or communicate the views of an individual or non-school sponsored organization; or to raise funds for any non-school-sponsored purpose, whether for-profit or not-for-profit. No employee shall knowingly provide school e-mail addresses to outside parties whose intent is to communication with school employees, students, and/or families for non-school purposes. Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from the building principal or other appropriate administrator.

6. Any communication that represents personal views as those of the school unit or that could be misinterpreted as such;

7. Downloading or loading software or applications without permission from the system administrator;

8. Opening or forwarding any e-mail attachments (executable files) from unknown sources and/or that may contain viruses;

9. Sending mass e-mails to school users or outside parties for school or non-school purposes without the permission of the system administrator [or other designated administrator];

10. Any malicious use or disruption of the school unit's computers, networks and Internet services or breach of security features;

11. Any misuse or damage to the school unit's computer equipment;

12. Misuse of the computer passwords or accounts (employee or other users);

13. Any communications that are in violation of generally accepted rules of network etiquette and/or professional conduct;

14. Any attempt to access unauthorized sites;

15. Failing to report a known breach of computer security to the system administrator;

16. Using school computers, networks and Internet services after such access has been denied or revoked; and

17. Any attempt to delete, erase or otherwise conceal any information stored on a school computer that violates these rules.

18. The Augusta School Department staff and administrators **may not self-provision cloud services to store, process, share, or manage data**. Regulated institutional data are data that are regulated by information privacy or protection laws, regulations, contracts, binding agreements (such as non-disclosure or data use agreements), or industry requirements. If your office is looking to provision a cloud service to support its work, it should consult with IT support. If your department or office needs to provision a cloud service to store, process, share, or otherwise manage regulated institutional data, it must work with the IT Department in order to properly evaluate and manage the risks that come with using the service for regulated institutional data. This will help ensure that agreements with cloud service providers have the appropriate provisions, such as notification of changes to the service's protective measures and assurance that the service properly destroys deleted data.

D. No Expectation of Privacy

The school unit retains control, custody and supervision of all computers, networks and Internet services owned or leased by the school unit. The school unit reserves the right to monitor all computer and Internet activity by employees and other system users. Employees have no expectation of privacy in their use of school computers, including e-mail messages and stored files.

E. Confidentiality of Information

Employees are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential.

F. Staff Responsibilities to Students

Teachers, staff members and volunteers who utilize school computers for instructional purposes with students have a duty of care to supervise such use. Teachers, staff members and volunteers are expected to be familiar with the school unit's policies and rules concerning student computer and Internet use and to enforce them. When, in course of their duties, employees/volunteers become aware of student violations, they are expected to stoop the activity and inform the building principal. [or other appropriate administrator].

G. Compensation for Losses, Costs and/or Damages

The employee shall be responsible for any losses, costs or damages incurred by the school unit related to violations of policy GCSA and/or these rules.

H. School Unit Assumes No Responsibility for Unauthorized Charges, Costs or Illegal Use

The school unit assumes no responsibility for any unauthorized charges made by employees including but no limited to credit card charges, subscriptions, long distance telephone charges, equipment and line costs, or for any illegal use of its computers such as copyright violations.

Adopted: January 12, 2000

Revised: January 14, 2015