Computer Control Policy

The District’s Computer Control Policy is formulated in accordance with the District’s Internet Use Agreement, and reflects the following principles:

• Security and integrity of District networks, hardware, software and information resources are important considerations
• District equipment and resources are to be used in support of job specific needs and the educational process

The Computer Control Policy includes the following components:

• Data Center Access, Security, Reporting, Monitoring and Backups
• Staff and Student Access to District Computers and Networked Resources
• Software

Data Center

➢ Access
  ▪ Data center is locked at all times with key entry to limited personnel

➢ Physical security of computer resources is also provided in the computer room by:
  ▪ Power control: generator back-up
  ▪ Temperature control with automatic email and phone alerts
  ▪ Only authorized Systems staff are allowed to access servers, where access includes:
    ▪ Stopping and starting; rebooting.
    ▪ Managing, modifying or otherwise using system and administration files.
    ▪ Performing back-ups.

➢ Reporting problems
  ▪ All other staff, will refer server problems or concerns to authorized Systems staff for resolution. No non-Systems staff is allowed to access administration or system files or to physically handle, in any way, data center servers.

➢ Monitoring System Security for Servers
  ▪ The Network Administrator and Network Backup are responsible for monitoring usage logs for root access.

➢ Back-ups for shared resources
  ▪ Complete data backups are performed daily on all servers. Data is stored off-site, at various locations throughout the District.
Staff and Student Access to District Computer and Networked Resources

- Staff use of mail server for email accounts and work-related file storage

- Staff accounts are immediately terminated and passwords immediately deleted when a staff member terminates employment with the District. Upon termination of employment, as a courtesy, the Systems Department contacts the terminating staff member and informs him/her that his/her email account will be disabled in two weeks.

- Physical security for most staff computers are provided by general building security measures, such as keycard-accessible staff areas, video cameras

- The District may provide staff members with computer equipment for their use in the performance of their job. It is understood that this equipment is borrowed and always remains the property of the District. In order to borrow equipment staff members must complete the Computer Equipment Sign-Out Form. (see attached)

Software

- All software installed on District-owned computers must be authorized software purchased and installed by the District Technology Department. All software is purchased and maintained by the Technology Department in compliance with the licensing agreement provided at time of purchase by the manufacturer or reseller. Staff may not use any personal or unauthorized software on District-owned computers.