Policy Level: TECHNOLOGY SERVICES	Rescinds Code:	Descriptor Code:
Descriptor Term: DATA AND NETWORK RESOURCES SECURITY POLICY/PLAN	Effective Date: July 1, 2007	

Risk Assessment

The electronic network utilized by faculty, students, and staff of the Fayette County Board of Education must be protected from unlawful invasion and malicious destruction. Data gathered to document student performance, staff functions, communications, and business activities now requires a need for protection and assurance of accuracy.

The Family Educational Rights and Privacy Act may deny federal funding to any educational agency which releases student records or personally identifiable information regarding any student without adopting adequate security policies. In Georgia, the right to privacy is a fundamental right protected by the state constitution and federal statutory law, 15 U.S.C. sections 6501-6502 which prohibit websites or online services from collecting personal information from children without obtaining permission from parents.

Records with regard to mental health communications, child abuse records, child drug abuse records and AIDS records are all protected as confidential under various state and federal laws. Therefore, the Fayette County Board of Education herein documents detailed policies and plans to protect electronic records and systems of operation. Systems shall include, but shall not be limited to, wide area networks, local area networks, servers, computers, software, e-mail, student performance records, staff records, and any other means of electronic transmission.

Assessment of Vulnerability

All physical facilities shall be reviewed for proper security (door locks, alarm systems, etc.). Passwords shall be assigned for staff access to appropriate communication/network access. E-mail passwords shall be assigned from a random six-character generator. Passwords shall not be visible or adjacent to any computer on the network, i.e. sticky note on monitor or under keyboard. No student performance data or staff evaluation data shall reside on a laptop computer anywhere in the system.

The Fayette County Board of Education network shall be protected by a firewall, web filter system and malware protection system. Temporary access through the firewall may be provided. Appropriate software for detection of password changes and lessening of network security measures shall be maintained.

Data to be Protected

All student data shall be protected. Should data become corrupt or manipulated, any performance judgments regarding students or the school system would be deemed unusable. Hardware and software used for electronic means in the system must be protected, as well. Malware protection software must be maintained and up-to-date at all times. Access to servers and network administration areas must be limited to appropriate personnel only.

Software shall not be copied for personal use and all software utilized in the system shall have proper licensing prior to use. Copying software violates copyright laws

Staff and student folders stored on servers or other electronic storage devices shall have separate areas, servers, and/or access. All access shall be through properly assigned passwords.

Further, all access to the Internet shall follow the guide of the Children's Internet Protection Act, the acceptable use policies as established by the Fayette County Board of Education, and only after having properly signed acceptable use policies. Filtering and blocking will be utilized in the network to prevent inappropriate access to non-educational, inappropriate Internet sites.

Acceptable Use Policies

Acceptable use policies (Student Acceptable Use Policy and Staff Acceptable Use Policy) will be maintained and updated as necessary for both student and staff use of the network, Internet, and electronic communication capabilities of the network.

Violation of the acceptable use policy by students may terminate network/Internet privileges and disciplinary procedures documented in the Guidelines for Student Behavior will be followed.

Violations by staff of the acceptable use policy may result in termination of privileges, reprimand, suspension, or termination from employment based on the infraction and the situation of the abuse of the policy.

Access Issues

All student data shall be accessible only by authorized personnel. Likewise, all personnel records shall be accessible only by authorized personnel. Data integrity shall be maintained to ensure accuracy of all data and reporting. Periodic audits shall be performed such as FTE counts and reviews of backup tapes for actual data saved for restoration.

Business Continuity

All data shall be backed up daily and system data backed up weekly. Weekly data tapes shall be stored in fireproof vaults in each facility and financial data will be stored in the county office vault. Reciprocity of operating systems (another business/school system) shall be procured to ensure business continuity in the case of a catastrophic event (tornado, hurricane, etc.).