STUDENT INFORMATION SYSTEM ACCEPTABLE USE

Policy Code: **3221**

The Asheboro City Schools Board of Education has the legal and ethical responsibility to collect, use and disseminate appropriate student information. The legal aspects of the use of public school data are based upon state and federal laws, including the Uniform Education Reporting System (UERS) umbrella as required by GS 115C-12. Additionally, the Family Educational Rights and Privacy Act (FERPA) mandates procedures for protecting the privacy of student data, while acknowledging the necessity to collect it. North Carolina further defines the situations in which both student and education student data can be disclosed in GS 115C and State Board of Education Policy EEO-C-017.

The following will govern the use of the student information system adopted by North Carolina Department of Public Instruction in the Asheboro City Schools.

Purpose

The purpose of this standard is to reduce unauthorized access to information within the student information system.

Application

All student information system users are required to read and follow this policy concerning user identification (user ID), password protection, and workstation standards.

Policy – User ID and Password Standards

- Each user accessing the student information system shall be uniquely identified with an ID that is associated only with that user.
- The LEA student information system administrator, or designee, is responsible for promptly disabling the student information system user ID upon termination of a user from the school or LEA or upon cessation of a user's need to access the student information system.
- Unsuccessful login attempts shall be limited to three (3) attempts before the user account is locked from access.
- Only authorized security administrators shall be allowed to enable a user ID.
- Passwords used for the student information system should be unique to the student information system.
- Passwords will expire every one hundred and twenty (120) days.
- No student information system passwords should be written or stored in clear text on or around the desktop systems.
- Passwords cannot be shared with any other person. Each user is personally responsible for all data entered and activity under her/his user ID.

Areas of Responsibility

All information maintained by the student information system is confidential. Any employee who violates the confidentiality of the records may be subject to disciplinary action.

Each principal is responsible for enforcing and monitoring the implementation of this policy.

The Superintendent, or designee, is responsible to ensure this policy is communicated to all student information system users.

Legal References: The Family Educational Rights and Privacy Act Statute (20 UCS § 1232g); Regulations-34 CFR Part 99

Adopted: May 12, 2005

Revised: September 11, 2014