

NCWISE PASSWORD AND WORKSTATION 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 as one of its most important priorities. The legal aspects of the use of public school data are based upon several 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) as amended in 1996, 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 (and cannot) be disclosed in GS 115C and State Board of Education Policy EEO-C-017.

The North Carolina Window of Information on Student Education (NCWISE) is the state's selected system for student accounting and collection and reporting of student information. The following will govern the use of NCWISE in the Asheboro City Schools.

Purpose

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

Application

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

Background

This policy has been based on the guidelines of the Information Resource Management Commission (IRMC) policy set forth by the Department of Public Instruction while outlining specific guidelines for its own technology environment. The use of passwords in conjunction with unique user IDs is required in order to allow authorized access to the NCWISE information. It is intended to prohibit the possibility of compromising student information and to maintain the integrity, accuracy, and confidentiality of the student data for the school district.

Scope

This policy applies to anyone using the NCWISE application per State Board Policy EEO-C-018.

Policy – User ID and Password Standards

- Each user accessing the NCWISE application shall be uniquely identified with an ID that is associated only with that user.
- The LEA security administrator, or his/her designee, is responsible for promptly disabling the NCWISE user ID upon termination of a user from the school or LEA or upon cessation of a user's need to access the NCWISE system.
- Unsuccessful login attempts shall be limited to three (3) attempts before the user logon

process is disabled.

- User IDs that are inactive for thirty (30) days will be disabled.
- Only authorized security administrators or help desk staff shall be allowed to enable a user ID.
- Passwords used for the NCWISE system should be unique to NCWISE.
- Passwords will expire every ninety (90) days.
- No NCWISE passwords should be written or stored in clear text on or around the desktop systems.
- **PASSWORDS CANNOT BE SHARED WITH ANYONE. EACH USER IS PERSONALLY RESPONSIBLE FOR ALL DATA ENTRY UNDER HIS/HER USER NAME.**

Workstation Security Standards

- A. Users should not login using NCWISE user identification to a public access computer. This includes, but is not limited to computer labs, cyber cafes, coffee shops, bookstores, libraries, etc.
- B. Anti-virus software should be installed on each desktop computer, and designated staff shall make certain that the desktop has the most current anti-virus software and appropriate updates installed. Users should update the virus protection software weekly to avoid unwanted viruses or damage that can be caused by them.
- C. Users should never leave the computer unattended while logged into NCWISE. The site must be locked using the feature built into the software.
- D. Only approved software should be installed on an NCWISE-designated computer.
- E. Browsers should be configured so that passwords for websites are not stored in the browser.
- F. Users should watch for keystroke monitors. These are small devices, less than an inch in size, which can be plugged in between the keyboard cable and the CPU. They record every character typed (including passwords) and save them in a text file or send them to a remote user.
- G. Workstation must be protected by a firewall.
- H. Users must create a separate user profile for students to use the NCWISE-designated computer.
- I. Accessing NCWISE from home will be permitted if the user can meet standards B, C, E and G above.

Areas of Responsibility

All information maintained by NCWISE 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 his/her designee is responsible to ensure this policy is communicated to all NCWISE users.

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

Adopted: May 12, 2005

Administrative Procedure: None