DATA PRIVACY AND NCSIS USER POLICY *Policy Code:* 3231

Employees of Wilkes County Schools are responsible for maintaining the integrity, accuracy, and confidentiality for all school district data. All users accessing confidential information are required to read and follow this policy concerning user identification (user ID), password protection, and workstation standards.

- All users accessing confidential information must sign the school district's Acceptable Use Policy.
- All personnel will follow federal, state, and local laws and regulations regarding sensitive and confidential material.
- Authorized personnel will use the Wilkes County Schools' assigned employee login when accessing the NC Student Information System (NCSIS).
- Teachers are responsible for recording absences. The principal's designee will maintain absence reason codes. Absence excuses will be filed in the office.
- Teachers are solely responsible for recording grades in NCSIS.
- To maintain password security, users must access applications from a secure workstation. A secure workstation is free of viruses, spyware, or any other malicious software.
- NCSIS Coordinators are responsible for enabling NCSIS logins at the school level.
- Passwords used for accessing confidential information should be unique.
- Requesting another's passwords is prohibited.
- Passwords should never be shared. Never store passwords in clear text where they can be easily viewed or found. If you think your password has been compromised, immediately report the incident to the principal and ITF.
- Personal information should never be inserted into email messages or any other forms of electronic communication. This includes social security numbers, driver's license number, passwords, etc.
- User logins will be disabled when it is no longer necessary to receive access to information.
- Antivirus software will be installed and maintained on all Wilkes County Schools' computers.
- Only approved software should be installed on computers.
- Computers exhibiting suspicious activity should be shut down until evaluated by the

technology department.

- Teachers should immediately report, in writing, to the ITF or principal any suspicious activity occurring on a computer accessing confidential information. This includes reports of viruses, spyware, password hacking, or any other irregularities.

- North Carolina has chosen to make NCSIS available to users via the Internet. Wilkes County Schools' employees may access NCSIS from computers outside the Wilkes County Schools' secure network, however, users must ensure the computers accessing NCSIS have the following current Anti-Virus software with up to date virus definitions.

If using wireless connectivity, the user is responsible for ensuring the wireless router is properly configured to be a secure transmission. Computers exhibiting suspicious activity must not be used. Employees must take proper precautions to ensure the confidentiality of student information is upheld while using computers inside or outside the school network.

- Wilkes County Schools is not responsible for maintaining computers outside the school network. Staff members are responsible for acquiring the proper software and technical support for these computers.

- Wilkes County Schools will not be held liable for damage to other systems due to outside use. Wilkes County Schools will also not be held liable for sensitive information being made public as a result of outside use.

- Violators may face financial restitution for damages. They may also face prosecution if *Family Educational Rights and Privacy Act* (FERPA) is violated.

Legal References: 20 U.S.C. 1232g; 34 CFR Part 99 (FERPA), GS 147-33.111

Adopted: November 7, 2005

Revised: January 4, 2007, April 6, 2009, March 3, 2014