LUZERNE INTERMEDIATE UNIT #18

SECTION: OPERATIONS

TITLE: ELECTRONIC STUDENT RECORDS ACCESS

ADOPTED: NOVEMBER 18, 2015

	815.1. Electronic Student Records Access
1. Purpose 20 U.S.C. Sec. 1232 (g) 34 CFR 99	The Family Educational Rights and Protection Act of 1974 requires intermediate units to protect student and family privacy by controlling unauthorized access to student records. Student medical and educational records are now be aggregated in central databases which are potentially accessible to staff through any networked computer. The underlying principle of FERPA is that individual student records may only be viewed by staff with a medical, psychological, educational, administrative, or other need to know. Summary records or reports should not identify individual students. This policy uses a combination of informational and technological safeguards.
2. Definition	This policy emphasizes, but is not limited to, student records in computer databases. The term **student records** shall refer to educational, medical, psychological, and any other records protected by law such as records of family income. Only educational and medical records are being placed in centralized, network-accessible, computer databases.
3. Guidelines	<u>Informational Components</u> All eligible staff will be informed about acceptable and unacceptable uses of student records before they may access student records electronically. A signed statement from each staff member that they have read and understand the policy will be kept on file. The opening screens of all computerized student records systems will contain the following warning, or its equivalent: Warning: You are permitted to access the educational (medical, etc.) records of individual students only if you have a job-related need-to-know; accessing individual student records without such a need-to-know illegal under the Federal Family Educational Rights and Protection Act (FERPA). All access to individual student records is logged and regularly monitored. Violators are subject to disciplinary and/or legal action. Annual informational sessions (e.g., at faculty meetings) will update staff on the confidentiality and protection of student information, including electronic access issues.

	Technological Components **Physical security** – Computers housing centralized student records will be located in a physically secure location (e.g., Data Processing and Technology Departments) accessible only to authorized staff. **Password security -** Access to databases of student records will be protected by individual staff passwords. These passwords will be secure, unguessable passwords of at least six (6) characters containing a mandatory mix of letters, numbers, and punctuation characters. **Transmission security -** The electronic transmission of student records and access passwords shall migrate to a system of secure, encrypted communication as such technology systems become practical, reliable, and affordable. **Levels of access** – Access to specific student information will be granted according to the need-to-know of the user's category. For example, a nurse's password will grant access to only medical records, and a teacher's password will grant access to only educational records. Certain office and technical staff require access to student records as part of their jobs. Secretaries, for example, need access to a student's immunization record, but no other medical information. To the degree practical, electronic systems will provide access only to needed information. The student records from specialized data systems such as food service systems, library systems, integrated learning systems, etc., will be accessible to the appropriate users of those systems. **Access logging**- All computer access to centralized individual student records will be logged to provide an audit trail that records the date and time of each staff member's access to each individual educational and medical record. The logs will be saved to a secure computer and will be archived for at least one (1) year. **Access monitoring –** Access logs to student records will be regularly monitored to verify need-to-know compliance. Reports of individual staff access to student data may be produced to confirm suspected activity.