800-800.1
ADMISTRATIVE PROCEDURE

ELECTRONIC DATA STORAGE

ERIE COUNTY TECHNICAL SCHOOL

ADOPTED: March 2023

	ELECTRONIC DATA STORAGE
1. Purpose	The ECTS Joint Operating Committee is committed to the secure management of the district's electronic data to ensure the confidentiality, integrity, and the availability of the data for all district users. Electronic data is aligned to the district's Record Management Policy.
2 Delegation of Responsibility	The Director shall develop procedures to implement this policy and shall delegate to their designee(s) the right to enforce this policy.
3. Definitions	**Sensitive Electronic Data** – electronic data stored by the District that includes student records, employee records, financial records, and any other confidential or sensitive information. **Transitory Electronic Data** – temporary electronic data not regularly stored by the District including, but not limited to, website cookie data, social media posts, live chat, deleted messages, and video surveillance that has not been purposefully saved. **Personal Information** - An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted: (i) Social Security number. (ii) Driver's license number or a State identification card number issued in lieu of a driver's license. (iii) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account. (iv) Medical information. (v) Health insurance information.

4. Guidelines Policy 800 Records Management Policy; Policy 800.1 Electronic Signatures/ Records	(vi) A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account. <u>Data Security Controls</u> The Information Technology Director, or their designee, shall utilize appropriate technical controls including firewalls, virus/malware detection, network access controls, user access controls, intrusion detection systems, encryption, and/or regular software updates to maintain the integrity and security of all the District's electronic data. <u>Access Controls</u> Sensitive electronic data shall be accessible to individual users on a need-to-know basis only. The Information Technology Director, or their designee, shall ensure that technical controls are utilized to effectively restrict access to sensitive electronic data to individuals with a legitimate educational or operational purpose to access such data. <u>Backups</u> The Information Technology Director, or their designee, shall ensure that the District maintains regular and up-to-date backups of all sensitive electronic data, and that such back-ups are stored either offline or are sent to secure off-site storage. <u>Vendors</u> The District may engage vendors who will have access to sensitive electronic data. In such cases, the Information Technology Director, or their designees, shall ensure that the vendor is required to adhere to the same data security standards as outlined in this policy, and shall ensure the appropriate provisions in the vendor contract to ensure compliance. <u>Data Storage</u> Sensitive electronic data may only be stored in secure storage approved by the District. The Information Technology Director shall maintain a list of approved storage options for sensitive electronic data and shall disseminate such list at least annually to all staff and administrators. <u>Retention</u> Sensitive electronic data shall be retained in accordance with the District's record retention policy and record retention schedule. Transitory electronic data shall only be maintained as delineated in the record retention schedule. <u>Personal E-mail</u> Personal e-mail accounts (accounts not issued by the District) shall not be used to transmit the District's sensitive electronic data in any way (including e-mailing files to/from one's own District e-mail account). <u>Personal Electronic Devices</u> Employees should exercise caution and utilize appropriate security measures such as password protection on their personal electronic device, to prevent any unauthorized access to sensitive electronic data. In no case shall employees store sensitive electronic data locally on the hard drive or internal memory of the employee's personal electronic device.

Policy 815 Acceptable use of Internet	<u>Data Breach</u> Any actual or suspected data breach (including unauthorized access to sensitive electronic data or exceeding one's authorization to electronic data) must be immediately reported to the Information Technology Director. Any data breach that results in unauthorized access to unredacted and unencrypted personal information shall be immediately reported to the Information Technology Director. The Director, or their designee shall follow the notification procedures required by the Breach of Personal Information Notification Act.
73 Pa. Stat. §2301 et seq.	<u>Risk Assessments</u> The Information Technology Director shall conduct regular vulnerability and risk assessments to monitor compliance with this policy. <u>Penalties for Violations</u> Violations of this policy, other Board policies, administrative regulations, and/or state or federal laws, including unauthorized access to sensitive electronic data, will result in discipline, up to and including dismissal. If appropriate, referrals will be made to law enforcement officials. <u>Development of Administrative Guidelines</u> The Information Technology Director or their designee may develop administrative guidelines to implement this policy. The Information Technology Director shall ensure that all students and employees are made aware of this policy and any administrative guidelines by means of the employee and student handbooks, the school district website, or other reasonable means.