Information Security and Incident Response

It is vital to the Tredyffrin Easttown School District that information security incidents that threaten the confidentiality, integrity or availability of the District's digital assets, information systems, network, and sensitive information contained thereon be properly identified, contained, investigated, and remedied.

Consistent with state and federal law and regulations, the District shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure of sensitive personal information collected or maintained in the regular course of business.

This Policy applies to students, staff, and contractors (generally referred to in this Policy as "users") of the District and to all other persons accessing the District's computer/network resources or information assets stored on or accessible via those resources, regardless of whether such resources or assets are accessed from on-campus or off-campus locations. This Policy is also applicable with respect to computing or network devices owned, leased, or otherwise controlled by the District. It is also applicable to any computing or network device, regardless of ownership, on which restricted or confidential information is stored or by which access to restricted or confidential information might be gained.

In the event that the Superintendent or their designee discovers a breach of the security of a system maintained by the District that contains personal information as defined in the accompanying Administrative Regulation, the Superintendent or their designee will provide appropriate notice of such breach under the standards set forth in this policy and accompanying regulation.

Delegation of Responsibility

The Superintendent or designee shall work with the appropriate administrative staff and the District's Solicitor to develop Administrative Regulations implementing this policy to ensure the District's ongoing engagement with cybersecurity best practices and to address the manner in which the District will respond to unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the District.