Hewlett-Woodmere Public Schools **Policy 8135**

( ) Required
(x) Local
( ) Notice

Instructional Technology Systems: Disaster Recovery Plan

The Board of Education recognizes its responsibility to safeguard the District's technology and computer systems in case of an emergency.

Hewlett-Woodmere Public Schools shall develop and maintain updated plans, operating procedures and redundant instructional technology, data management, operational, financial, emergency communication and information technology systems to be followed in the event of natural or manmade disasters or enemy attack (the "Disaster Recovery Plan"). The administration will implement the Disaster Recovery Plan by using a variety of appropriate and effective strategies such as proactively establishing redundant server systems, third party contract agreements for hosted software and a third data memory- storage facility located off Long Island. The goal of implementing this policy will be to safeguard the vital information of the Hewlett-Woodmere Public Schools, to allow the timely and effective continued operation of all aspects of its operations, and to reduce the risk of delayed or interrupted computer operations and prevent the loss of equipment and data.

The Disaster Recovery Plan will align with state and federal cybersecurity standards, including the National Institute Standards and Technology (NIST) Cybersecurity Framework and New York State Education Department (NYSED) guidelines. The District will conduct periodic cybersecurity risk assessments and implement multi-factor authentication (MFA), encryption protocols, and continuous network monitoring to protect against unauthorized access and data breaches.

A listing of the critical operational functions requiring the use and support of instructional technology systems and services will be reviewed by the Superintendency each year. The Superintendency will develop regulations describing the responsibilities and attach the regulations to this policy. The regulations will identify the members of the leadership team who are responsible for ensuring that specific assigned critical instructional, informational, management and communication systems and services are in place, tested on a regular basis and functional.

A listing of the critical functions and a confidential summary description of the strategies implemented to fulfill the requirements of this policy will be shared and reviewed with the Board of Education.

Due to the confidential nature and security priority of the Disaster Recovery Plan(s), specific chapters of the plan will be classified and identified as confidential and intended for internal use only. The Disaster Recovery Plan(s) will be updated annually to incorporate any changes in the technology environment.

Approved: June 16, 2010
Amended: April 16, 2024, May 14, 2025