HEWLETT-WOODMERE UFSD **Policy 8630**

( ) Required
(X) Local
( ) Notice

TECHNOLOGY RESOURCES AND DATA MANAGEMENT

The Board of Education recognizes that technology is a powerful and valuable education resource and research tool and as such is an important part of the instructional program. In addition, the district depends upon technology as an integral part of administering and managing the schools' resources, including the compilation of data and recordkeeping for personnel, students, finances, supplies and materials. This policy outlines the Board of Education's expectations in regard to these different aspects of the district's technology resources.

This policy covers all users of technology, and all other technologies, that may provide access to the Internet and/or other networks within or linked to the School District (the School District's "technology resources"). Technology resources provide the School District, its personnel, and students with unique opportunities for the sharing of knowledge, information and ideas that can positively impact ~~the~~ instructional and organizational programs. With access to the School District's technology resources comes the responsibility for proper online conduct, acceptable use of the network, proper use of copyrighted material, and sanctions for inappropriate use.

General Provisions

The Superintendent shall be responsible for designating an Assistant Superintendent for Teaching, Learning, and Technology who will oversee the use of district technology resources. The Assistant Superintendent for Teaching, Learning, and Technology will prepare in-service programs for the training and development of district staff in technology skills, appropriate use of technology and for the incorporation of technology use in subject areas.

The Superintendent, working in conjunction with the designated purchasing agent for the district, and Assistant Superintendent for Teaching, Learning, and Technology will be responsible for the purchase and distribution of technology software and hardware throughout the schools. They shall prepare and submit for the Board's approval a comprehensive multi-year technology plan which shall be revised as necessary to reflect changing technology and/or district needs.

The Superintendent, working with the Assistant Superintendent for Teaching, Learning, and Technology, shall establish regulations governing the use and security of the district's technology resources (technology resources include all devices that process data, including but not limited to, laptops, fax machines, copiers and scanners). The security and integrity of the district technology network and data is a serious concern to the Board and the district will make every reasonable effort to maintain the security of the system. All users of the district's technology resources shall comply with this policy and regulation, as well as the district's policy 4526, Network and Technology Acceptable Use Policy. Failure to comply may result in disciplinary action, as well as suspension and/or revocation of technology access privileges. Unauthorized tampering or mechanical alteration including software configurations will be considered vandalism, which is prohibited and illegal.

Further, all student users of the district's technology resources will have access according to his/her assigned rights, with appropriate authorization and parent consent either in writing or digitally. District devices and accounts must only be used for school-related purposes. All users of the district's technology resources must understand that use is a privilege, not a right, and that use entails responsibility. Users of the district's network must not expect, nor does the district guarantee, privacy for electronic mail (e-mail) or any use of the district's network. The district reserves the right to access and view any material stored on district equipment or any material used in conjunction with the district's network.

<u>Management of Technology Records</u>

The Board recognizes that since District data is maintained digitally, it is critical to exercise appropriate control over technology records, including financial, personnel and student information. The Superintendent, working with the Assistant Superintendent for Teaching, Learning, and Technology and the District's business official, shall establish procedures governing management of digital records: taking into account whether the records are stored onsite on district servers or on remote servers in the "cloud". The procedures will address:

- passwords,
- system administration,
- separation of duties,
- remote access,
- encryption,
- user access and permissions appropriate to job titles and duties,
- disposal of technology equipment and resources (including deleting district data or destroying the equipment),
- inventory of technology resources (including hardware and software),
- data back-up (including archiving of e-mail),

- record retention, and
- disaster recovery plans and notification plans.
- multi-factor authentication

If the district contracts with a third-party vendor for services that require access to district digital resources and/or data, the Superintendent, in consultation with Assistant Superintendent for Teaching, Learning, and Technology**,** Business Official, and School Attorney, will ensure that all agreements will comply with the management of digital records.

Review and Dissemination

Since technology is a rapidly changing area, it is important that this policy be reviewed annually by the Board of Education and the district's internal and external auditors. The regulation governing appropriate technology use will be distributed annually to staff and students and will be included in both employee and student handbooks.

Cross-ref: 5300, Code of Conduct
1120, School District Records
4526, Network and Technology Acceptable Use
4526.1, Internet Safety
5500, Student Records
6600, Fiscal Accounting and Reporting
6700, Purchasing
6900, Disposal of District Property
8635, Information Security Breach and Notification

Adoption date: July 6, 2022

Amended: July 5, 2023

HEWLETT-WOODMERE UFSD **Regulation 8630-R**

TECHNOLOGY RESOURCES AND DATA MANAGEMENT REGULATION

The following rules and regulations govern the use of the district's network employee access to the Internet, and management of technology records.

I. Administration

- The Superintendent of Schools shall designate an Assistant Superintendent for Teaching, Learning, and Technology to oversee the district's network.
- The Assistant Superintendent for Teaching, Learning, and Technology or his/her designee shall monitor and examine all network activities, as appropriate, to ensure proper use of the system.
- The Assistant Superintendent for Teaching, Learning, and Technology shall maintain an updated inventory of all technology hardware and software resources.
- The Assistant Superintendent for Teaching, Learning, and Technology shall develop and implement procedures for data back-up and storage. These procedures will facilitate the disaster recovery and notification plan and will comply with the requirements for records retention in compliance with the district's policy on School District Records (1120).
- The Assistant Superintendent for Teaching, Learning, and Technology shall be responsible for disseminating and interpreting district policy and regulations governing use of the district's network at the building level with all network users.
- The Assistant Superintendent for Teaching, Learning, and Technology shall provide employee training for proper use of the network and will ensure that staff supervising students using the district's network provide similar training to their students, including providing copies of district policy and regulations (including policy 4526, Network and Technology Acceptable Use Policy) governing use of the district's network.
- The Assistant Superintendent for Teaching, Learning, and Technology shall take reasonable steps to protect the network from viruses, other software, and network security risks that would compromise the network or district information.
- All student and employee agreements to abide by district policy and regulations and parental consent forms shall be kept on file either in the district office or digitally.
- Consistent with applicable internal controls, the Superintendent in conjunction with the school business official and the Assistant Superintendent for Teaching, Learning, and Technology will ensure the proper segregation of duties in assigning responsibilities for technology resources and data management.

II. Internet Access

Student Internet access is addressed in policy and regulation 4526, Network and Technology Acceptable Use. District employees and third party users are governed by the following regulations:

- Employees will be issued an e-mail account through the district's network.
- Employees are expected to review their e-mail daily on a regular basis.
- Communications with parents and/or students should be saved as appropriate and the district will archive the e-mail records according to procedures developed by the Assistant Superintendent for Teaching, Learning, and Technology.
- Employees may access the internet for education-related and/or work-related activities.
- Employees shall refrain from using technology resources for personal use.
- Employees are advised that they must not have an expectation of privacy in the use of the district's technology.
- Use of technology resources in ways that violate the acceptable use and conduct regulation, outlined below, will be subject to discipline.

III. Acceptable Use and Conduct

The following regulations apply to any use of the district's technology systems:

- Access to the district's network is provided solely for educational and/or research purposes and management of district operations consistent with the district's mission and goals.
- Use of the district's network is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege.
- Each individual in whose name an access account is issued is responsible at all times for its proper use.
- All network users will be issued a login name and password. Passwords must be changed periodically and must be of sufficient complexity as determined by the district.
- Only those network users with permission from the Assistant Superintendent for Teaching, Learning, and Technology may access the district's system from off-site (e.g., from home).
- All network users are expected to take reasonable precaution to secure district information stored on devices they use, including maintaining responsible custody over technology resources, ensuring no unauthorized use of district devices, and exercising prudent judgement when browsing the internet and opening email.
- All network users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive language, vulgarities and swear words are all inappropriate.
- Network users identifying a security problem on the district's network must notify appropriate staff. Any network user identified as a security risk or having a history of violations of district technology use guidelines may be denied access to the district's network.

IV. Prohibited Activity and Uses

The following is a list of prohibited activity for **any user** concerning use of the district's network. Any violation of these prohibitions may result in discipline or other appropriate penalty, including suspension or revocation of a user's access to the network.

- Using the network for commercial activity, including advertising.
- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the district technology network.
- Using the network to receive, transmit or make available to others obscene, offensive, or sexually explicit material.
- Using the network to receive, transmit or make available to others messages that are racist, sexist, abusive or harassing to others.
- Use of another's account or password.
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users and deliberately interfering with the ability of other system users to send and/or receive e-mail.
- Forging or attempting to forge e-mail messages.
- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy district equipment or materials, data of another user of the district's network or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a technology virus, malware on the network, and not reporting security risks as appropriate.
- Using the network to send anonymous messages or files.
- Revealing the personal address, telephone number or other personal information of oneself or another person.
- Using the network for sending and/or receiving personal messages.
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software, using personal disks, or downloading files on the district's technology and/or network without the permission of the appropriate district official or employee.
- Using district technology resources for fraudulent purposes or financial gain
- Stealing data, equipment or intellectual property.
- Gaining or seeking to gain unauthorized access to any files, resources, or technology or phone systems, or vandalize the data of another user.
- Wastefully using finite district resources.
- Changing or exceeding resource quotas as set by the district without the permission of the appropriate district official or employee.
- Using the network while your access privileges are suspended or revoked.
- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.
- Exhibiting careless behavior with regard to information security (e.g., sharing or displaying passwords, leaving technology equipment unsecured or unattended, etc.).
- Using the network to receive, transmit or make available to others a message that is inconsistent with the District's Code of Conduct.

V. No Privacy Guarantee

- Users of the district's technology network should not expect, nor does the district guarantee, privacy for electronic mail (e-mail) or any use of the district's technology network. The district reserves the right to access and view any material stored on district equipment or any material used in conjunction with the district's technology network.

VI. Sanctions

- All users of the district's technology network and equipment are required to comply with the district's policy and regulations governing the district's technology network. Failure to comply with the policy or regulation may result in disciplinary action as well as suspension and/or revocation of technology access privileges.

- Illegal activity is strictly prohibited. Any information pertaining to or implicating illegal activity will be reported to the proper authorities. Transmission of any material in violation of any federal, state and/or local law or regulation is prohibited. This includes, but is not limited to materials protected by copyright, threatening or obscene material or material protected by trade secret. Users must respect all intellectual and property rights and laws.

VII. District Responsibilities

- The district makes no warranties of any kind, either expressed or implied, for the access being provided. Further, the district assumes no responsibility for the quality, availability, accuracy, nature or reliability of the service and/or information provided. Users of the district's technology network and the Internet use information at their own risk. Each user is responsible for verifying the integrity and authenticity of the information that is used and provided.

- The district will not be responsible for any damages suffered by any user, including, but not limited to, loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by the user's own negligence or any other errors or omissions. The district also will not be responsible for unauthorized financial obligations resulting from the use of or access to the district's technology network or the Internet.

- The district will take reasonable steps to protect the information on the network and provide a secure network for data storage and use, including ensuring that contracts with vendors address data security issues and that district officials provide appropriate oversight. Disposal of district technology resources shall ensure the complete removal of district information, or the secure destruction of the resource. Even though the district

- The District may use technical and/or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of the district policy and regulation.

Adoption date: July 6, 2022

Amended: July 5, 2023