SUBJECT: STAFF ACCEPTABLE USE POLICY

The Board will provide staff with access to various computerized information resources through the District's computer system (DCS hereafter) consisting of software, hardware, computer networks, wireless networks/access, and electronic communication systems. This may include access to electronic mail, on-line services, and the Internet. It may also include the opportunity for staff to have independent access to the DCS from their home or other remote locations, and/or to access the DCS from their personal devices. All use of the DCS and the wireless network, including independent use off school premises and use on personal devices, will be subject to this policy and any accompanying regulations.

The Board encourages staff to make use of the DCS to explore educational topics, conduct research and contact others in the educational world. The Board anticipates that staff access to various computerized information resources will both expedite and enhance the performance of tasks associated with their positions and assignments. To that end, the Board directs the Superintendent or designee(s) to provide staff with training in the proper and effective use of the DCS.

Staff use of the DCS is conditioned upon written agreement by the staff member that use of the DCS will conform to the requirements of this policy and any regulations adopted to ensure acceptable use of the DCS. These agreements will be kept on file in the Technology Office.

Generally, the same standards of acceptable staff conduct which apply to any aspect of job performance will apply to use of the DCS. Employees are expected to communicate in a professional manner consistent with applicable District policies and regulations governing the behavior of school staff. Electronic mail and telecommunications will not be utilized to share confidential information about students or other employees.

Access to confidential data is a privilege afforded to District employees in the performance of their duties. Safeguarding this data is a District responsibility that the Board takes very seriously. Consequently, District employment does not automatically guarantee the initial or ongoing ability to use mobile or personal devices to access the DCS and the information it may contain.

This policy does not attempt to articulate all required and/or acceptable uses of the DCS; nor is it the intention of this policy to define all inappropriate usage. Administrative regulations will further define general guidelines of appropriate staff conduct and use as well as proscribed behavior.

District staff will also adhere to the laws, policies, and rules governing computers including, but not limited to, copyright laws, rights of software publishers, license agreements, and rights of privacy protected by federal and state law.

Staff members who engage in unacceptable use may lose access to the DCS and may be subject to further discipline under the law and in accordance with applicable collective bargaining agreements. Legal action may be initiated against a staff member who willfully, maliciously, or unlawfully damages or destroys property of the District.

(Continued)

SUBJECT: STAFF ACCEPTABLE USE POLICY (Cont'd.)

Social Media Use by Employees

Philosophy Statement

To meet the challenges of preparing students for the future, the District must explore new and emerging technologies to supplement learning and communication opportunities for students, parents, teachers, and staff. This includes the use of social networking sites (SNS). SNS have great potential to connect people across the world and enhance communication; they are also more informal, less structured, and still emerging.

Social media are powerful communication devices that have a significant impact on business, organizational, and professional reputations. Because they tend to blur the line between personal and professional positions, however, the District has adopted these guidelines to avoid abuse or misuse of the media, to protect personal and professional information and reputations, and to establish some basic parameters on the creation and use of SNS for the District and its personnel.

Definition of Social Networking Sites

Social networking sites are web sites or online communities that connect people through social interaction and other networks. Social networking sites often include a range of communication platforms including, but not limited to, creation of profiles, blogs, discussion boards, instant messaging, and file sharing. Some examples of SNS are Facebook, My Space, Twitter, YouTube, LinkedIn, Instagram, Snap Chat, and Vine.

The District's Social Networking Site

Any form of school-related social networking will be restricted to the District's website and authorized third party SNS. Personal use of social media or SNS by employees on District time or on District-owned equipment is prohibited. School personnel, mainly the faculty who publish to and maintain an instructional web site with blogging capabilities, will be included in the DSNS. Access to the DSNS for matters related to school business or educational activities may be permitted as authorized by the employee's supervisor.

The Superintendent or designee will have the exclusive and final authority to determine whether individual groups such as elementary, middle, or high school students may initiate and maintain separate pages(s) on the DSNS.

Quality Control/Content Integrity

The District's official web site will remain the primary source for all published content related to District news, events, information, and all other information and data related to the District. The District strictly prohibits school personnel from publishing content about the North Warren Central School District and making reference to students or other personnel on any other site.

(Continued)

SUBJECT: STAFF ACCEPTABLE USE POLICY (Cont'd.)

The District will provide general training, including training on ethical, legal considerations, and compliance with all applicable policies and regulations for all personnel on use of the DSNS.

Ethical Standards/Legal Obligations

District personnel must conduct themselves in the virtual or online world of DSNS or personal SNS just as they would in all face-to-face interactions, namely, treating others with dignity and respect and observing all other established standards of professional conduct. Any party on a social media site or responding to posts must be respectful. On any SNS, it is expected that District personnel will present themselves in a professional way to project a positive appearance as a District employee.

District personnel acknowledge and agree that when they create or post material on the DSNS, they are, in effect, content publishers, and thus are subject to a number of ethical and legal obligations including, but not limited to, compliance with the federal Digital Millennium Copyright Act.

Employees must not post confidential or proprietary information about the District, its students, employees, or alumni. In addition, employees must adhere to all applicable state and federal laws, including, but not limited to, FERPA and HIPAA. Employees must also adhere to all District privacy and confidentiality policies. Privacy does not exist in the social media world. The impact of a specific post may reflect poorly on employees and the District. If it is something that an employee would not say at a conference or to the administration, it should not be posted.

While mindful of employees' First Amendment free speech rights, District personnel who participate in social networking web sites, including the DSNS or any public SNS, will not post material which may result in the disruption of classroom or District activities, as determined by the District.

The Superintendent or designee, in conjunction with the Technology Department, will monitor the DSNS to encourage uses to contribute accurate, valuable, and high-quality information on the DSNS.

Due to the evolving nature of these primarily social web sites, District personnel should not use SNS to create or maintain personal relationships with students, which means any behavior or conduct that is unrelated to course work or official school matters. Inappropriate behavior may erode the professional authority and traditional roles of teacher and student within the District and may violate District policies or regulations. Employees must not connect on any SNS with any current student of the District with the exception of their own children or an immediate family member's child.

Social media sites must be identified as the employee's own and not as a representative of the District, unless previously authorized to do so. Employees must not use District logos or any other District images or iconography on any personal social media site, unless previously authorized to do so. In addition, the District's name must not be used to promote a product, cause, political party, or candidate.

(Continued)

SUBJECT: STAFF ACCEPTABLE USE POLICY (Cont'd.)

Confidential or private data, including, but not limited to, protected student records, employee personal identifying information, and District assessment data, will only be loaded, stored, or transferred to District-owned devices which have encryption or password protection. This restriction, designed to ensure data security, encompasses all computers and devices within the DCS, any mobile devices, including flash or key drives, and any devices that access the DCS from remote locations. Staff will not use email to transmit confidential files in order to work at home or another location. Staff will not use personal cloud-based storage services (such as Dropbox, GoogleDrive, SkyDrive, etc.) for confidential files.

In addition, staff will not leave any devices unattended with confidential information visible. All devices must be locked down while the staff member steps away from the device, and settings enabled to freeze and lock after a set period of inactivity.

Staff data files and electronic storage areas will remain District property, subject to District control and inspection. The Technology Coordinator may access all staff data files and communications without prior notice to ensure system integrity and that users are complying with requirements of this policy and any accompanying regulations. Staff should not expect that information stored on the DCS is private.

Reporting Requirements

District personnel are required to report known or suspected violations of this policy to a District administrator or supervisor.

Disciplinary Sanctions

District personnel who violate any provision of this policy are subject to appropriate disciplinary measures up to and including termination of employment in accordance with legal guidelines, District policy and regulations, and any applicable collective bargaining agreement.

NOTE: Refer also to Policies #5672 -- Information Security Breach and Notification
#6411 -- Use of Email in the District
#7243 -- Student Data Breaches
#7316 -- Student Use of Personal Technology
#8271 -- Internet Safety/Internet Content Filtering Policy

Adoption Date: August 13, 2018