**SUBJECT: ACCESS AND USE OF COMPUTERIZED INFORMATION RESOURCES
            (INTERNET)**

Staff Use of Computerized Information Resources

The Board of Education of the Pine Valley Central School District will provide staff access to various computerized information resources through the District's Computer System (DCS hereafter) consisting of software, hardware, computer networks and electronic communication systems. This may include access to electronic mail, so called "on-line services" and the "Internet." It may include the opportunity for some staff to have independent access to the DCS from other remote locations. All use of the DCS, including independent use off school premises, shall be subject to this policy.

One purpose of this policy is to provide notice to students, parents and guardians and staff that, unlike most traditional instructional or library media materials, the DCS will allow access to external computer networks not controlled by the School District where it is impossible for the District to screen or review all of the available materials. Some materials may be deemed unsuitable for use or access by anyone utilizing the DCS. This policy is intended to establish guidelines and regulations for staff to follow in instruction and in working with students on acceptable student use when there will be access to external computer networks.

Generally, the same standards of acceptable staff conduct that apply to any aspect of job performance shall apply to the use of the DCS. Staff members who engage in unacceptable use may lose access to the DCS and may be subject to further discipline under the applicable procedures and/or applicable contractual guidelines. Legal action may be initiated against a staff member who willfully, maliciously or unlawfully damages or destroys property of the District or of others.

In addition to the general requirements of acceptable staff behavior expected under the District's school conduct and discipline policy, staff shall be prohibited from engaging in any of the following:

a) Using the DCS to obtain, view, download, send, print, display, or otherwise gain access to or to transmit materials that are unlawful, obscene, pornographic, abusive;

b) Damaging, disabling, or otherwise interfering with the operation of computers, computer systems, software or related equipment through physical action or by electronic means;

c) Using unauthorized software on the DCS;

d) Changing, copying, renaming, deleting, reading, or otherwise accessing files or software not created by the staff members without expressed permission from the system administrator;

e) Violating copyright law or employing the DCS for any commercial purpose;

(Continued)

SUBJECT: ACCESS AND USE OF COMPUTERIZED INFORMATION RESOURCES (INTERNET) (Cont'd.)

 f) Disclosing an individual password to others or using others' passwords;

 g) Use of the DCS for other than school related work or activities;

 h) Assisting a student to violate District policy or failing to report knowledge of any student violations of the District's policy regarding student use of computerized information resources;

 i) Use of obscene or vulgar language;

 j) Harassing, insulting, or attacking others;

 k) Use of the DCS in any unlawful manner.

   Staff data files and other electronic storage areas are School District property subject to control and inspection by the District. School officials may access all such files and communications to ensure system integrity, to ensure that users are complying with the requirements of this policy and for other reasons. Staff should NOT expect that information stored on the DCS will be private.

Social Media Use by Employees

   The School District recognizes the value of teacher and professional staff inquiry, investigation and communication using new technology tools to enhance student learning experiences. The School District also realizes its obligations to teach and ensure responsible and safe use of these new technologies. Social media, including social networking sites, have great potential to connect people around the globe and enhance communication. Therefore, the Board of Education encourages the use of District approved social media tools and the exploration of new and emerging technologies to supplement the range of communication and educational services.

   For purposes of this Policy, the definition of **public social media networks or Social Networking Sites (SNS**) are defined to include: websites, Web logs (blogs), wikis, social networks, online forums, virtual worlds, and any other social media generally available to the School District community which do not fall within the District's electronic technology network (e.g., Facebook,

(Continued)

**SUBJECT: ACCESS AND USE OF COMPUTERIZED INFORMATION RESOURCES
(INTERNET) (Cont'd.)**

MySpace, Twitter, LinkedIn, Flickr, blog sites, etc.). The definition of **District approved password-protected social media tools** are those that fall within the District's electronic technology network or which the District has approved for educational use. Within these internal forums, the District has greater authority and ability to protect minors from inappropriate content and can limit public access.

The use of social media (whether public or internal) can generally be defined as Official District Use, Professional/Instructional Use and Personal Use. The definitions, uses and responsibilities will be further defined and differentiated in the Administrative Regulation. The School District takes no position on an employee's decision to participate in the use of social media or SNS for personal use on personal time. However, personal use of these media during District time or on District-owned equipment is prohibited. In addition, employees are encouraged to maintain the highest levels of professionalism. They have responsibility for addressing inappropriate behavior or activity on these networks, including requirements for mandated reporting and compliance with all applicable District Policies and Regulations.

The Superintendent is authorized to establish regulations and procedures as necessary to implement the terms of this policy.

Student Use of Computerized Information Resources

The Board of Education of the Pine Valley Central School District will provide student access to various computerized information resources through the District's computer system (DCS hereafter) consisting of software, hardware, computer networks and electronic communication systems. This may include access to electronic mail, so called "on-line services" and the "Internet". It may include the opportunity for some students to have independent use off school premises, which shall be subject to this policy.

Access to Inappropriate Content/Material and Use of Personal Technology or Electronic Devices

This policy is intended to establish general guidelines for the acceptable student use of the DCS and also to give students and parents/guardians notice that student use of the DCS will provide student access to external computer networks not controlled by the School District. The District cannot screen or review all of the available content or materials on these external computer networks. Thus some of the available content or materials on these external networks may be deemed unsuitable for student use or access by parents/guardians.

Despite the existence of District policy, regulations and guidelines, it is virtually impossible to completely prevent access to content or material that may be considered inappropriate for students. Students may have the ability to access such content or material from their home, other locations off school premises and/or with a student's own personal technology or electronic device on school grounds or at school events. Parents and guardians must be willing to establish boundaries and

(Continued)

SUBJECT: ACCESS AND USE OF COMPUTERIZED INFORMATION RESOURCES (INTERNET) (Cont'd.)

standards for the appropriate and acceptable use of technology and communicate these boundaries and standards to their children. The appropriate/acceptable use standards outlined in this policy apply to student use of technology via the DCS or any other electronic media or communications, including by means of a student's own personal technology or electronic device on school grounds or at school events. The District respects the right of each family to decide whether to allow their child independent computer access.

Student access to the DCS will automatically be provided unless the parent has submitted written notification to the District that such access not be permitted. Procedures will be established to define the process by which parents may submit a written request to deny or rescind student use of the DCS in accordance with law, Commissioner's Regulations and/or District policies and procedures.

Generally, the same standards of acceptable student conduct that apply to any school activity shall apply to the use of the DCS.

District students shall also adhere to the laws, policies and rules governing computers and iPads including, but not limited to, copyright laws, rights of software publishers, license agreements, and student rights of privacy created by federal and state law. The District's Acceptable Use Policy and regulations will be disseminated to parents and students in order to provide notice of the school's requirements, expectations and student's obligations when accessing the DCS.

Students who engage in unacceptable use may lose access to the DCS in accordance with applicable due process procedures, and may be subject to further discipline under the District's school conduct and discipline policy and the Student Discipline Code of Conduct. The District reserves the right to pursue legal action against a student who willfully, maliciously or unlawfully damages or destroys property of the District or another person. The District may bring suit in civil court against the parents or guardians of any student who willfully, maliciously or unlawfully damages or destroys District property pursuant to Education law 1709(36).

Student data files and other electronic storage areas will be treated like student school lockers. This means that such areas are School District property subject to control and inspection. School officials may access all such files and communications to ensure system integrity, to ensure users are complying with the requirements of this policy and for other reasons. Students should NOT expect that information stored on the DCS will be private.

In addition to the general requirements of acceptable student behavior expected under the District's school conduct and discipline policy, students shall be prohibited from engaging in any of the following:

 a) Using the DCS to obtain, view, download, send, print, display, or otherwise gain access to or to transmit materials that are unlawful, obscene, pornographic, abusive;

(Continued)

SUBJECT: ACCESS AND USE OF COMPUTERIZED INFORMATION RESOURCES (INTERNET) (Cont'd.)

b)   Damaging, disabling, or otherwise interfering with the operation of computers, computer systems, software or related equipment through physical action or by electronic means;

c)   Using unauthorized software on the DCS;

d)   Changing, copying, renaming, deleting, reading, or otherwise accessing files or software not created by the student without expressed permission from the system administrator;

e)   Violating copyright law or employing the DCS for any commercial purpose;

f)   Disclosing an individual password to others or using others' passwords;

g)   Use of the DCS in any unlawful manner;

h)   Use of the DCS for other than school or educational activities.

The Superintendent is authorized to establish regulations and procedures as necessary to implement the terms of this policy.

NOTE: Refer also to Policy #8271 -- Internet Safety/Internet Content Filtering Policy
                       #8273 -- Use of Email in the School District

Adopted: 11/30/06
Revised: 6/7/12; 4/22/14