SUBJECT: ELECTRONIC INFORMATION NETWORK (EIN) AND INTERNET SAFETY

The Pittsford Central School District Electronic Information Network and Internet Access Policy (EIN) is the overriding policy from which these regulations are derived. These regulations apply, but are not limited to, Web pages, social networking sites, video posting sites, podcasts, wikis, and blogs. EIN Users agree to follow the rules and responsibilities as outlined below and the federal Digital Millennium Copyright Act.

Students and staff are provided an account on the District's Electronic Information Network. The use of the EIN is a privilege, not a right. Therefore, the District can, at its own discretion, withhold, rescind, or terminate such use at any time, for any reason. Access to the network is provided to facilitate resource sharing, innovation, and communication. EIN computer systems and software, including communications and information transmitted by, received from, or created in these systems are the exclusive property of the District. Electronic storage areas (e.g., browser logs and other memory banks) are District property, and are subject to District control and inspection. The District will periodically monitor those logs and memory banks. Therefore, data stored on the EIN is not private. Messages or other data relating to or in support of illegal activities will be reported to the authorities.

Value Statement

To accommodate new communication tools and remain at the forefront of preparing students for the future, educators and school districts shall explore new and emerging technologies and their applications for stakeholders. These stakeholders may include Board members, parents, students, teachers, staff, media, and the community at large.

Content

Content Integrity

The Board of Education and the administration encourage the development of Web pages by staff members in order to provide information to parents, students, and the community about classroom and student activities as well as instructional resources. To be considered an authorized Website, Web pages must be developed in accordance with this regulation using resources consistent with the District's Web presence and using only District-sanctioned tools, links, and Websites

Family Educational Rights and Privacy Act (FERPA)

Confidential information regarding students, staff, or the organization may not be posted on Web pages, including but not limited to directory information under FERPA. (See Policy 3320, Confidentiality of Computerized Information, and Policy 7240, Student Records: Access and Challenge.

.

(Continued)

SUBJECT: ELECTRONIC INFORMATION NETWORK (EIN) AND INTERNET SAFETY

In addition, the following guidelines apply to all Web pages developed by District staff and housed within Websites authorized by the District.

Quality Control

The official District Website will remain the primary source for all content. All Web pages must support the District's vision, mission, and goals; comply with District policies, regulations, and Web standards; be maintained with current, accurate, and well-written information; be reviewed and updated regularly; be grammatically and mechanically correct (except where original student work is to be displayed in original form); and be proofread using a browser to ensure correct editing.

Material/content entered or posted to the District sites and pages (e.g., Facebook, Twitter) must include a link back to the official District Website or relevant partner. An occasional reminder or announcement without a link is permissible (e.g., a "Save the Date" announcement).

As it relates to Policy #8310 "Purpose of Instructional Materials," all subject matter on the Web pages and their links must relate to curriculum and instruction, District-authorized activities and services, or information about the District or its mission.

Appropriate Content

Content is subject to District review. In order to be maintained, Web pages may require editing at the direction of the Administrator assigned to oversee the page(s). If a page is deemed inappropriate, it will be removed. The District reserves the right to determine what it considers to be inappropriate. Web page content and links covered by this document must include appropriate material. Examples of inappropriate actions/material may include, but are not limited to, modifying District Web pages, linking to District Web pages housed on the EIN without authorization, scanning images or making audio or video recordings without prior permission from the District or appropriate copyright permission (See Regulation 8271 R2-Web Page Design and Copyright Guidelines), commercial promotions, political lobbying, promotion of illegal acts, any material considered libelous or slanderous, any material that violates any PCSD Policy, and objectionable language.

District Level and Building Level Content

The District's Communications Office will establish and maintain the initial District's pages and sites (e.g., Facebook, Twitter) to further the public relations/outreach/connection to the District's various stakeholders and will monitor the content.

(Continued)

SUBJECT: ELECTRONIC INFORMATION NETWORK (EIN) AND INTERNET SAFETY

At the District level, pages pertain to District-wide information such as the District calendar or Curriculum, Departments, and Staff across the District. At the building level, pages are specific to the school building.

For example, the District calendar contains major events such as Superintendent Conference Days, Recess Dates, Performing Arts events, and Book Fairs. At the building level, calendar information may include more routine events such as roller skating parties, field trips, and club information.

Blogs, Podcasts, Wikis, Video Podcasts (Vodcasts), and other Social Networking Sites (SNS)

In addition to or as part of a Web page, staff may choose to create blogs, podcasts, wikis, and vodcasts to engage students in effective dialogue on selected topics. Staff members are expected to utilize Web 2.0 communication tools such as blogs, podcasts, and vodcasts that are developed in accordance with this regulation using resources provided by and hosted on sites consistent with the District's Web presence or the District's mission.

Staff who use blogs, podcasts, wikis or vodcasts as instructional tools should remember that their content may be viewed by anyone who has the ability to access the Website on which the content is located. Blogs, podcasts, wikis, and vodcasts should be reserved for instructional use only and be monitored closely by the staff member.

Students and staff members are responsible for the content of instructional blogs, podcasts, wikis, and vodcasts they create and staff members must include disclaimers within those personal blogs that the views are their own and do not reflect their employer. Instructional blogs, podcasts, and vodcasts will be monitored in the same manner as Web pages.

Inappropriate material may not be posted by staff or students. If inappropriate content is found, it will be removed immediately and notification will be made to the staff member who created the blog, podcast, wiki or vodcast.

Ethical Standards, Legal Obligations, and User Responsibilities

Ethical Standards and Obligations

1) District personnel and students shall conduct themselves in the "virtual" or online world just as they would in all face-to-face human interactions, namely treating others with dignity and respect and observing all other established standards of professional conduct. Also, personnel and students shall maintain the privacy of passwords and refrain from discussing or publishing passwords. Users of the EIN shall respect the privacy of the data of other EIN users. EIN users are prohibited from hacking, accessing or transmitting material that is profane or obscene, adult-oriented, or material that advocates illegal acts, violence, discrimination toward other people or material that advocates illegal acts, harassment or discrimination (Refer to Policy 7552-Student Harassment: Bullying: Peer Abuse in the Schools)

(Continued)

2) District personnel and students shall acknowledge and agree that when they create or post material on the District SNS they are in effect "content publishers" and as such are subject to a host of ethical and legal obligations including, but not limited to, compliance with the federal Digital Millennium Copyright Act and copyright laws.

3) The Director of Communications, in conjunction with the Technology Director, shall help facilitate the District Web pages and sites to encourage users to contribute accurate, valuable, and high-quality information.

4) While mindful of students' and employees' First Amendment free speech rights, District students and personnel who participate in social networking Websites shall not post any material that may result in the disruption of the classroom or District activities. The District is entitled to make such a determination based on the facts surrounding the material in question.

5) Due to the evolving nature of these primarily social Websites, District personnel should not use SNS, email, chat rooms or other forms of direct electronic communications to create or maintain personal relationships with students, or vice versa. For purposes of these guidelines, "personal relationships with students" shall mean any behavior or conduct that is unrelated to course work or official school matters. Such behavior may compromise the professional authority and traditional roles of teacher and student within the District and may violate District policies and/or regulations. EIN users are prohibited from attempting to disrupt the computer system, destroying data by spreading viruses or altering system software.

6) Access to SNS for personal, commercial, or for-profit purposes during the District's workday is prohibited. However, access to the District's Websites and pages for matters related to school business and/or educational activities is permitted as authorized by the employee's supervisor.

EIN User Expectations

EIN Users are responsible for attending appropriate training sessions in the use and care of hardware, software, and networks. Users are expected to refrain from using technology for which they have not received training or with which they are not competent.

Users are also responsible for scanning electronic media for viruses or physical contamination, which might endanger the integrity of District hardware, software or networks before they are used in District systems utilizing District tools and programs. Also, users shall review and, when appropriate, delete old, unwanted files.

District users shall not disrupt or degrade the performance of the network or other networks beyond the EIN.

(Continued)

SUBJECT: ELECTRONIC INFORMATION NETWORK (EIN) AND INTERNET SAFETY

Illegally installing copyrighted software for use on District computers or the EIN, loading unapproved software on computers, and attaching personal devices to the EIN without the expressed permission of a network administrator are prohibited. (See 8271 Regulations).

Reporting Requirements and Consequences

Students and personnel shall be required to report known or suspected violations of the District EIN Guidelines to their Building Principal or immediate supervisor.

Students who do not comply with the regulations stated in this document will lose computer/EIN privileges. Infractions may result in disciplinary action as outlined in the District Code of Conduct, Policy 3410, in addition to suspension or termination of access privileges.

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

Disclaimer of Responsibility

Users of any information obtained via the EIN is at the user's own risk. The District exercises no control over the content of the information residing on the EIN or passing through it. The District purchases its Internet service through a provider that filters inappropriate images.

Some websites may contain inappropriate or objectionable material for a minor, such as defamatory, inaccurate, abusive, profane, sexually oriented, threatening, racially offensive, or illegal material. Parents of minors having access to the Internet should be aware of the existence of such material and the ability of the student to access this material through the Internet, either at school or at home. As a result, the District disclaims any responsibility for inappropriate or objectionable materials that a student may obtain through the use of the Internet. Filtering software is not 100% safe. The District may, under certain circumstances, disable the blocking or filtering technology for adults and students engaged in bona fide research or other lawful purposes. This disabling may only be exercised by the Director of Technology or his/her designee and will remain disabled only for the period of time during which the research is being conducted.

Users of the EIN should not expect the information on the EIN will remain private. All data files and electronic storage areas shall remain District property and, as such, are subject to District control and inspection.

(Continued)

SUBJECT: ELECTRONIC INFORMATION NETWORK (EIN) AND INTERNET SAFETY

General Safety

Student Safety

Student names may be published, but should never be associated with information that would lead to the identification of a student. For example, posting a student's full name with a photograph, grades, course work, medical information or other specific information is prohibited, or if a photograph is used, it should never be coupled with identifying information like student's name, class, grade, etc. without specific parental permission.

Identifying information includes, but is not limited to name, phone number, e-mail address, age, and links to personal Web pages.

When uploading a file containing an approved photo, make certain the file name does not include students' names. Students' names could be inadvertently shared, accessed as part of the image's code. First re-save the photo using another generic description before uploading to the Web.

Student Privacy

Student personal information is restricted and privacy must be maintained. Personal and/or medical information may not be published in association with student name for public access. Personal information includes but is not limited to grades, competitive ranking, medical information, and sports clearances.

If you need to post restricted student information, contact the Director of Student Services at 267-1025.

Employee Privacy

The District will not post home or cell phone numbers or personal/home e-mail addresses of employees without their permission.

Compliance with Other Applicable Policies and Regulations

District users who participate in any online, social networking or Web posting shall be subject to all applicable policies and regulations per Pittsford's Board of Education.

Questions should be addressed to the District's Technology Office at 267-1082 or the Communications Office at 267-1031.

Physical Plant

No maps of school building layouts may be posted on the EIN.