# REGULATIONS FOR DISTRICT EMPLOYEES AND APPROVED THIRD PARTIES

## COMPUTER NETWORK RESPONSIBLE USE AND INTERNET SAFETY

The intent of this Responsible Use Regulation is to provide reasonable guidelines for the appropriate use of the District's *Network,* which includes Internet access, wireless Internet access, District e-mail accounts, computing and networking facilities, hardware and software. This Regulation assumes an attitude of cooperation, good will and appropriate *Network* "etiquette" on the part of District administrators, faculty, staff, students and approved third parties using our technology facilities.

Interpretation, application and modification of this Responsible Use Exhibit shall be within the sole discretion of the Hempstead School District.

It is the District's philosophy that students learn to use technology tools to communicate globally and to this end, it is essential that technology is integrated with instruction. In addition, information technology tools have become invaluable to teachers in delivering instruction, and to administrators, staff and approved third parties in supporting educational processes. As demand for Internet bandwidth increases for all users, priority will be given to instructional and curricula needs over personal use.

The District will comply with the Children's Online Privacy Protection Act (COPPA) and Family Educational Rights and Privacy Act (FERPA), and will follow and enforce the New York State Parents' Bill of Rights for Data Privacy and Security, and all other applicable laws. For data analyses and instructional decision-making purposes, certain District-wide software titles are presented to teachers, students and instructional support staff pre-populated with student data because they meet the following criteria:

1. They comply with the COPPA, FERPA and other laws;
2. The vendor has signed the Data Privacy Pledge, and/or
3. The software has been vetted by the District or BOCES

In adherence to these laws, while using teacher-selected online learning tools and games in the classroom, students' **Personal Identifiable Information (PII) <u>should not</u> be entered into these programs independently by teachers, staff, and third parties**.

Students' PII includes the following:

a) The student's name (first and last name);
b) The name of the student's parent or other family members;
c) The address of the student or student's family;

d) A personal identifier, such as the student's social security number, student number, or biometric record;
e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
g) Information requested by a person who the District reasonably believes knows the identity of the student to whom the education record relates.

**If software that is used independently by teachers calls for student PII information, aliases must be used. If a lookup file is maintained by the teacher to cross-reference the alias information, the file must be saved on the teacher's private (H:) drive on the network. This information cannot be shared electronically or printed.**

## Internet Filtering and Internet Safety

District filtering technology is configured to prevent access to material that is obscene, illegal, pornographic and/or that is harmful to minors, as defined by the Children's Internet Protection Act ("CIPA").

a) Teachers will provide students with a sequential, structured approach to gaining the skills that will allow them to become independent, responsible users of the *Network*.

b) Teachers will ensure that students are directed to sites with age and topic appropriate materials and resources as referenced in K-12 curriculum documents.

c) Users will be responsible for what they post to Blackboard webpages and District's websites.

d) Users may only post photographs of students to Blackboard and other class webpages or District websites if the parent(s) have signed a media release form and the staff member has verified it.

e) Users of non-District owned, i.e. personal, wired or wireless devices, including laptops, wireless broad-band network cards, Internet enabled cell phones, etc. shall not disrupt the educational process and users shall not access inappropriate or illegal material.

## Social Media

Social media has become a useful communication and collaboration tool and may be used responsibly for educational and promotional purposes. Social media includes all online interaction methods including but not limited to blogs, Office 365's Yammer and other

social network sites. The District has approved a limited number of social media sites for use by staff and third parties which are managed internally. The Dignity for All Students Act, the District's Code of Conduct and Policy (0115) on Bullying prevention prohibit cyberbullying and outline the District's responsibility to address incidents that take place in the District and outside the District that could disrupt the school environment.

a) Teachers', staff, and third parties' educational media accounts should be separated from personal.
b) Teachers, staff and third parties will not connect a personal social page with students.
c) Teachers, staff and third parties will only use District approved social media networks for instructional and student collaboration purposes.

**System User's Rights**

The District reserves the right to, and does, monitor the use of the District's *Network,* including District-owned computers, Internet access, wireless Internet access, e-mail accounts, computing and networking facilities, hardware and software and other related technologies. Therefore, students, staff and community members should have no expectation of privacy when they use the District's *Network*.

*Network* storage areas are District property. The administration may review files and communications at any time to maintain system integrity and insure that the system is being used in accordance with District policies and regulations. All material stored on District equipment shall be deemed District property.

The Hempstead School District reserves its right to disable any computer account and further, to conduct an investigation and/or review of *Network* usage, as well as to gain access to the user's correspondence and/or files without prior notice to the user.

**Responsible Use Guidelines**

a. The *Network* of the Hempstead School District (District) supports administrators, faculty and staff in instructional research, teaching, community-based presentations and other intellectual endeavors related to respective roles and responsibilities and consistent with the District's mission. Generally, any computing or network activities that fall within these categories are considered acceptable use of the District's Network.

b. All District administrators, faculty and staff have a responsibility to become familiar with the responsible use policies for students, and with specific guidelines and consequences for misuse of District technology, as more specifically set forth in student responsible use regulations and the District Code of Conduct, and to do their best to ensure adequate supervision to maintain executed student use agreements. The District has two student responsible use Regulations as follows: a) Elementary Responsible Use Regulation (Regulation 4526-E.1) and b) Middle/High School Responsible Use (Regulation 4526-E.2).

c. The holder of a District computer USER ID and password is required to sign for use of the *Network* and is responsible for protecting the *Network* from unauthorized access by keeping the password confidential and by changing it regularly and logging off from computers when not in use.

d. The holder of a District computer USER ID account shall be liable for any misuse of the *Network* which takes place using that account. Therefore, always log off.

e. Copyrighted material may not be placed on any computer connected to the District's *Network* without appropriate legal authorization. This includes but is not limited to copying, installing, receiving, transmitting or making available any copyrighted software or other related materials on the *Network.* Copyrighted materials shall only be used in accordance with the "fair use" doctrine of federal copyright law.

**Prohibited and Unacceptable Use**

**1. Illegal Activities and/or Unacceptable Uses**

a. Users may not attempt to gain unauthorized access to the District's *Network* including data or to any other computer system through the District's *Network,* or to go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files without authorization.

b. Teachers, staff and third parties may not share their network access with substitute teachers or with students. Substitute teachers' folders, with substitute guest log-in credentials, should be obtained from the schools' front office or computer aides.

c. Users may not disrupt or attempt to disrupt the District's *Network* performance or destroy data by spreading computer viruses or by any other means.

d. Users may not use the District *Network* for personal use, commercial use or political activity, including without limitation, school related matters, such as budget votes, referenda and Board elections, etc.

e. Users may not post chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to many people.

**2. Respecting Resource Limits**

a. Users shall use the *Network* only for educational or professional development activities related to their position in the District.

b. When possible, use other District-provided storage for networks for video content.

c. Users should check their e-mail at least at the beginning and end of each day and manage the size of mailbox storage.

**3. Accessing Inappropriate Material**

a. Users may not use the District *Network* to receive, access or distribute material that is profane, offensive, obscene, discriminatory, pornographic or otherwise sexually explicit or that advocates illegal acts, is defamatory, or that advocates violence towards people or animals. Users may not use the *Network* to engage in any illegal act.
b. If anyone inadvertently encounters inappropriate content, the individual should immediately report or e-mail the Technology Department with the details.

**Disclaimer**

The Hempstead School District makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the system will be error-free or without defect. The District will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for financial obligations arising through the use of the system. The District will not be held liable for any content already existing on personal wireless devices. Users seeking to utilize the District's wireless Internet service must register with the District and be provided with a user name and password prior to being granted wireless access. In addition, users will be required to accept the Mobile Device Management ("MDM") client on their personal device(s) prior to gaining wireless access.

The Director of Technology is responsible for *Network* operations, providing help and answering questions.

*References:*
Board of Education Policy 4526
Regulations 4526-E.1, E.2, E.3,
District Code of Conduct and Dignity for All Students Act, Education Law §801-a;
Education Law, Article 2
5695 Students and Personal Electronic Devices

Board Adoption Date: February 15, 2018