

COMPUTER NETWORK AND INTERNET ACCEPTABLE USE POLICY

The Board of Education will actively pursue making advanced technology and increased access to learning opportunities available to district students and staff. In accordance with federal law, Internet access in our schools will be mediated through the use of blocking and/or filtering software. Internet access will allow district students and staff to access and use information available on distant computers, communicate and share information with individuals or groups of other students and staff, and significantly expand the users' knowledge base.

Students and staff must understand and practice proper and ethical use. The following are conditions and rules for use:

A. Acceptable Use

1. Effective September 1, 2011, all district computer network users will be required to acknowledge that they have received and reviewed this policy upon logging on to the computer network.
2. Internet use facilitates communication in support of research and education by providing access to unique resources and the opportunity for collaborative work. In order to remain eligible as a user, all Internet access should support the educational objectives of the District.
3. Transmission of any material in violation of any United States or state regulation is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secret. Use for commercial activities by students is not acceptable. Use for product advertisement or political lobbying is also prohibited.

B. Privilege

Use of and access to the Internet is a privilege, not a right. Inappropriate use, including any violation of these conditions and rules, may result in cancellation of the privilege. The Board has the authority to determine appropriate use and may deny, revoke, suspend or close any user account at any time based upon its determination of inappropriate use by any user. Each student who receives an account will be responsible for that account and its usage. Therefore, under no circumstances should an account be shared with anyone other than the Instructional Technology Specialist. Each student will also be required to attend an orientation session with a district faculty member pertaining to the proper use of the network.

C. Monitoring

All users, staff and students alike, have no right to privacy or confidentiality when using the District's computer network and equipment. The District reserves the right to examine and archive all electronic correspondence, e-mail and records of internet activity for network management, compliance and/or records retention purposes. All e-mail and other electronically stored information may be subject to records retention requirements and/or disclosure, in accordance with applicable laws or as part of discovery proceedings in legal actions.

D. No Warranties

The Board makes no warranties of any kind, whether express or implied, for the service it is providing. The Board and district staff will not be responsible for any damages a user suffers. This includes loss of data resulting from delays, no-deliveries, mis-deliveries, or service interruptions caused by the district's negligence or by the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The Board specifically denies any responsibility for the accuracy or quality of information obtained through its services. All users need to consider the source of any information they obtain, and consider how valid that information may be.

E. Security

Security on any computer system is a high priority, especially when the system involves many users. Attempts to log-on to the Internet in the name of another individual will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the Internet.

F. The Superintendent of Schools or his/her designee shall establish regulations governing the use and security of the District's computer network, and shall establish implementing procedures to enforce the regulations. The procedures shall provide for the safety and security of students using electronic correspondence such as e-mail, chat rooms and instant messages (IMs); monitoring the online activities of students using the District's computers and equipment; and restricting student access to materials that are harmful to minors. All users of the District's computer network and equipment shall comply with this policy, its regulations and implementing procedures. Failure to comply may result in disciplinary action; suspension and/or revocation of computer access privileges; and potential legal action.

1st Reading May 28, 2002

2nd Reading and Adoption March 24, 2009 June 24, 2002

1st Reading February 24, 2009

2nd Reading and Adoption March 24, 2009

1st Reading July 5, 2011

2nd Reading and Adoption August 16, 2011

COMPUTER NETWORK AND INTERNET ACCEPTABLE USE REGULATION

A. Internet Etiquette

All users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

1. Be polite. Do not be abusive in your messages to others.
2. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Do not engage in activities which are prohibited under state or federal law.
3. Do not reveal your personal contact information as well as the address and telephone numbers of other students or colleagues.
4. Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities will be reported to the authorities and may result in the loss of user privileges.
5. Do not use the network in such a way that you would disrupt the use of the network by other users.
6. All communications and information accessible via the network should be assumed to be public property.

B. Prohibited Activity

Prohibited activities concerning use of the District's computer network include, but are not limited to, the following examples:

- Copying, installing, receiving, transmitting or making available any copyrighted software or material on the district computer network.
- Using the network to receive, transmit or make available to others any sexually explicit or obscene material.
- Using the network to receive, transmit or make available to others messages that are racist, sexist, hateful, threatening, offensive, bigoted, abusive or harassing to others.
- Transmitting any other material in violation of any federal, state and/or local law or regulation.
- Using another user's account or password.
- Attempting to read, delete, copy or modify the e-mail of other system users.
- Deliberately interfering with the ability of other systems users to send, receive or save e-mail.
- Forging or attempting to forge e-mail messages.
- Deleting or attempting to delete e-mail messages that the law requires districts to retain as district records.
- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy district equipment or materials, data or 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 intentionally permitting a computer virus to enter the network.
- Using the network to send anonymous messages or files.
- Using the network to receive, transmit or make available to others a message that is inconsistent with the District's Code of Conduct.

- Revealing the personal address, telephone number or other personal information of oneself or another person.
- Using the network for sending and/or receiving personal electronic correspondence, including e-mail or instant messages (IMs).
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software or using personal disks on the District's computers and/or network without the permission of the appropriate district official or employee.
- Using district computing resources for commercial activity, advertising, financial gain, fraud or political lobbying.
- Stealing data, equipment or intellectual property.
- Gaining or seeking to gain unauthorized access to any files, resources, or computer or phone systems, via hacking or any other unauthorized methods.
- Wastefully using finite district resources.
- Using the network while access privileges are suspended or revoked.
- Using the network in a fashion inconsistent with directions from teachers and/or other staff and generally accepted network etiquette.

C. Procedures for Use

Student users must always get permission from their instructors before using the Internet and follow written and oral instructions from their instructors

D. Encounters with Controversial Material

Users may encounter material which is deemed controversial in nature and which users, parents, teachers or administrators may consider inappropriate or offensive. The district has installed protective filtering software to prevent access to vulgar, obscene and inappropriate material. However, on a global network it is impossible to ensure that such content will not be encountered and an industrious user may discover controversial material. It is the users responsibility not to initiate access to such material. Further, it is the responsibility of users to notify teachers if and when such material is encountered so that further preventive steps can be taken to make such material inaccessible.

E. Parental Approval

The Building Principal is responsible for receiving signed parental approval form before students may access the Internet. Parental approval stays in effect while student is enrolled in the district or until the parent withdraws permission in writing.

F. Penalties For Improper Use:

All users of the District's computer network and equipment are required to comply with the District's policy and regulations governing the District's computer network. Failure to comply with the policy or regulation may result in disciplinary action, including verbal or written warnings; suspension or revocation of a user's access to the network; detention; and/or expulsion from school.

In addition, violations may result in civil and/or criminal liability beyond the District's own disciplinary measures. Any information pertaining to or implicating illegal activity will be reported to the proper authorities for appropriate legal action. All network users should be aware that misuse of the District's computer network may lead to liability for, among other things, harassment, trespass, defamation and copyright infringement.

G. District Records

E-mail and other electronically stored information that are created in the course of school district business and retained as evidence of official policies, decisions or actions are district records, subject to the records management and retention requirements under the Local Government Records Law, (e.g., Records Retention and Disposition Schedule, "Ed-1"), and subject to disclosure pursuant to the Freedom of Information Law (FOIL) unless they fall within a statutory exception. Examples of district records contained in electronically stored information include:

- Policies and directives;
- Correspondence or memoranda related to school district business;
- Work schedules and assignments;
- Agendas and minutes of meetings;
- Non-final drafts of documents that are circulated for comment or approval;
- Documents that initiate, authorize or complete a business transaction; and
- Final reports or recommendations.

By contrast, examples of e-mail and other electronically stored information that are not district records include:

- Extra copies of documents;
- Personal messages or telephone message notifications;
- Social event announcements; and
- Copies or summaries of documents distributed for convenience or reference.

H. Electronic Information Used by School Board Members

The Board discourages its members from using any electronic communications to deliberate in their capacities as board members. In addition, Board members must not engage in any series of electronic communications that results in a collective decision, (such as a vote taken by e-mail.)

Nonetheless, the Board recognizes that any electronic correspondence by and between school board members and/or administrators that is used to communicate with each other in their capacities as board members or administrators are district records; shall receive the same diligent record-keeping treatment as all other district records; and may be subject to disclosure.

I. Electronic Record-Keeping Information Used by School Board Members

All school personnel and board members are expected to file and retain any e-mail or electronically stored information that is a district record under the definition set forth above. After so filing, users shall dispose of superfluous copies of e-mail and other electronically stored information in a timely manner.

All school personnel and board members are expected to regard any e-mail or electronic record containing any information that is personally identifiable to any student as a confidential student record in accordance with the Family Education Rights and Privacy Act (FERPA).

All school personnel and board members are expected to regard any e-mail or electronically stored information that constitutes a public record as subject to disclosure under FOIL unless they fall within a statutory exception.

Cross-Ref: 4526.1, Internet Safety

Legal Ref:

FERPA, 20 U.S.C. Section 1232g et seq; 34 C.F.R. Part 99

Children's Internet Protection Act, 47 U.S.C. Section 254 and 20 U.S.C. Section 9134;47 C.F.R. Part 54

Local Government Records Law., N.Y. Arts and Cultural Affairs Law, Article 57-A

FOIL, N.Y. Public Officers Law, Article 6

NY Education Law Section 814

Records Retention and Disposition Schedule, N.Y.C.R.R. Appendix I

United States vs. Am. Library Ass'n. 539 U.S. 194 (2003)

1st Reading May 28, 2002 2nd Reading & Adoption June 24, 2002

1st Reading for Re-Adoption: February 24, 2009

2nd Reading and Re-Adoption: March 24, 2009

INTERNET ACCEPTABLE USE EXHIBIT*Parental consent*

If you would like your child to be permitted to have Internet access via our library connection, please read and explain the above policy, regulation and agreement on Internet Acceptable Use to your child and sign the agreement below. These sign-off sheets should be returned to your school's main office.

Part I

I understand the above conditions and rules in the Internet Acceptable Use Policy and Regulation. I further understand that any violation of the above conditions, rules, and Acceptable Use Agreement may result in the loss of access privileges and/or disciplinary and/or appropriate legal action for those violating these conditions.

I hereby give permission for my child, _____, to access the Internet.

Parent or Guardian _____

Signature: _____

Date: _____

Part II

I have read the Internet Acceptable Use policy, regulation and agreement. I understand that this access is designed for educational purposes. I also recognize that while protective measures including filtering software have been put in place it is impossible for Valley Stream UFSD 13 and its employees to guarantee that access to controversial materials will not take place and I will not hold them responsible for my child accessing such materials on the Internet. Further, I am aware that there are commercial services available on the Internet and any charges incurred by me or my child regarding such services will be my responsibility and not the district's. I also release the Board and the district from any and all claims of damages of any nature arising from my, or my child's use, or inability to use, the system. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting.

I hereby give permission for my child, _____, to participate in Internet access in school.

Parent or Guardian: _____

Signature: _____

Date: _____

PART III – Publication of student’s work

I understand that my child’s work may be published on the Internet for non-commercial purposes, and I hereby give my permission for such publication of my child’s work. I also understand that my child will be identified by first name only.

My permission stays in effect while my child is enrolled in District 13 or until I withdraw my permission in writing to the building principal.

Parent Or Guardian: _____

Signature: _____

Date: _____

PART IV – Student Agreement

Parents – Please read and explain the terms outlined in this agreement with your child. Child and Parent signatures are required.

When using the Internet I agree that I will follow all of the rules listed below:

1. When I write to other people using the Internet I will remember to be polite and never write anything to hurt someone else’s feelings.
2. I will not use bad language such as cursing or name calling.
3. When I use the Internet, I will not give out my name, address, phone number or any information about myself or people I know to anyone.
4. I will not try to do anything that will cause damage to the computer.
5. If I encounter inappropriate material in the use of the Internet, I will alert a teacher.

I understand and will abide by the district’s Internet Acceptable Use policy, regulation and agreement. I further understand that any violation of the district’s policy is unethical and may constitute a criminal offense. Should I commit a violation, my access privileges may be revoked, school disciplinary actions may be taken, and/or appropriate legal action.

Student Name

Signature

I have read and discussed these rules with my child:

Parent/Guardian Name

Signature

1st Reading May 28, 2002

2nd Reading & Adoption June 24, 2002

1st Reading for Re-Adoption February 24, 2009

2nd Reading for Re-Adoption March 24, 2009

INTERNET SAFETY POLICY

The Board of Education is committed to undertaking efforts that serve to make safe for children the use of district computers for access to the Internet and World Wide Web. To this end, although unable to guarantee that any selected filtering and blocking technology will work perfectly, the Board directs the Superintendent of Schools to procure and implement the use of technology protection measures that block or filter Internet access by:

- adults to visual depictions that are obscene or child pornography, and
- minors to visual depictions that are obscene, child pornography, or harmful to minors, as defined in the Children's Internet Protection Act.

Subject to staff supervision, however, any such measures may be disabled or relaxed for adults conducting bona fide research or other lawful purposes, in accordance with criteria established by the Superintendent or his or her designee.

The Superintendent or his or her designee also shall develop and implement procedures that provide for the safety and security of students using electronic mail, chat rooms, and other forms of direct electronic communications; monitoring the online activities of students using district computers; and restricting student access to materials that are harmful to minors.

In addition, the Board prohibits the unauthorized disclosure, use and dissemination of personal information regarding students; unauthorized online access by students, including hacking and other unlawful activities; and access by students to inappropriate matter on the Internet and World Wide Web. The Superintendent or his or her designee shall establish and implement procedures that enforce these restrictions.

The Instructional Technology Specialist designated under the district's Computer Network or Acceptable Use Policy, shall monitor and examine all district computer network activities to ensure compliance with this policy and accompanying regulation. He or she also shall be responsible for ensuring that staff and students receive training on their requirements.

All users of the district's computer network, including access to the Internet and World Wide Web, must understand that use is a privilege, not a right, and that any such use entails responsibility. They must comply with the requirements of this policy and accompanying regulation, in addition to generally accepted rules of network etiquette, and the district's Acceptable Use Policy. Failure to comply may result in disciplinary action including, but not limited to, the revocation of computer access privileges.

4526.1

Cross-ref: 4526, Internet Acceptable Use

Ref: Public Law No. 106-554
47 USC §254
20 USC §6801

Legal Ref:

FERPA, 20 U.S.C. Section 1232g et seq; 34 C.F.R. Part 99
Children's Internet Protection Act, 47 U.S.C. Section 254 and 20 U.S.C. Section 9134;47
C.F.R. Part 54
Local Government Records Law., N.Y. Arts and Cultural Affairs Law, Article 57-A
FOIL, N.Y. Public Officers Law, Article 6
NY Education Law Section 814
Records Retention and Disposition Schedule, N.Y.C.R.R. Appendix I
United States vs. Am. Library Ass'n. 539 U.S. 194 (2003)

1st Reading May 28, 2002

2nd Reading & Adoption June 24, 2002

1st Reading for Re-Adoption February 24, 2009

2nd Reading for Re-Adoption March 24, 2009

INTERNET SAFETY POLICY REGULATION

The following rules and regulations implement the Internet Safety Policy adopted by the Board of Education to make safe for children the use of district computers for access to the Internet and World Wide Web.

I. Definitions

In accordance with the Children's Internet Protection Act,

- *Child pornography* refers to any visual depiction, including any photograph, film, video, picture or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. It also includes any such visual depiction that (a) is, or appears to be, of a minor engaging in sexually explicit conduct; or (b) has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or (c) is advertised, promoted, presented, described, or distributed in such a manner than conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.
- *Harmful to minors* means any picture, image, graphic image file, or other visual depiction that (a) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (b) depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (c) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

II. Blocking and Filtering Measures

- The Superintendent or his or her designee shall secure information about, and ensure the purchase or provision of, a technology protection measure that blocks access from all district computers to visual depictions on the Internet and World Wide Web that are obscene, child pornography or harmful to minors.
- The district's computer network coordinator shall be responsible for ensuring the installation and proper use of any Internet blocking and filtering technology protection measure obtained by the district.
- The computer network coordinator or his or her designee may disable or relax the district's Internet blocking and filtering technology measure only for adult staff members conducting research related to the discharge of their official responsibilities.

- The computer network coordinator shall monitor the online activities of adult staff members for whom the blocking and filtering technology measure has been disabled or relaxed to ensure there is not access to visual depictions that are obscene or child pornography.

III. Monitoring of Online Activities

- The district's computer network coordinator shall be responsible for monitoring to ensure that the online activities of staff and students are consistent with the district's Internet Safety Policy and this regulation. He or she may inspect, copy, review, and store at any time, and without prior notice, any and all usage of the district's computer network for accessing the Internet and World Wide Web and direct electronic communications, as well as any and all information transmitted or received during such use. All users of the district's computer network shall have no expectation of privacy regarding any such materials.
- Except as otherwise authorized under the district's Computer Network or Acceptable Use Policy, students may use the district's computer network to access the Internet and World Wide Web only during supervised class time, study periods or at the school library, and exclusively for research related to their course work.
- Staff supervising students using district computers shall help to monitor student online activities to ensure students access the Internet and World Wide Web, and/or participate in authorized forms of direct electronic communications in accordance with the district's Internet Safety Policy and this regulation.
- The district's computer network coordinator shall monitor student online activities to ensure students are not engaging in hacking (gaining or attempting to gain unauthorized access to other computers or computer systems), and other unlawful activities.

IV. Training

- The district's Instructional Technology Specialist shall provide training to staff and students on the requirements of the Computer Network and Internet Safety Policy and regulations
- The training of staff and students shall highlight the various activities prohibited by the Internet Safety Policy, and the responsibility of staff to monitor student online activities to ensure compliance therewith.
- Students shall be directed to consult with their classroom teacher if they are unsure whether their contemplated activities when accessing the Internet or Worldwide Web are directly related to their course work.

- Staff and students will be advised to not disclose, use and disseminate personal information about students when accessing the Internet or engaging in authorized forms of direct electronic communications.
- Staff and students will also be informed of the range of possible consequences attendant to a violation of the Internet Safety Policy and this regulation.

V. *Reporting of Violations*

- Violations of the Internet Safety Policy and this regulation by students and staff shall be reported to the Building Principal.
- The Principal shall take appropriate corrective action in accordance with authorized disciplinary procedures.
- Penalties may include, but are not limited to, the revocation of computer access privileges, as well as school suspension in the case of students and disciplinary charges in the case of teachers.

Adopted June 24, 2002

1st Reading for Re-Adoption February 24, 2009

2nd Reading for Re-Adoption March 24, 2009

INTERNET ACCEPTABLE USE AND SAFETY
Employee Agreement

Employee Name _____

Title _____

School/Office _____

I have read and understand the District’s “Internet Acceptable Use” and “Internet Safety” policies and regulations, and I agree to abide by their provisions. The District has taken precautions to restrict access to prohibited materials, but it is my responsibility not to initiate access to such material.

I understand that I have no right to privacy or confidentiality when I use the District’s computer network and equipment. I consent to district staff monitoring my electronic correspondence and records of Internet activity for network management, compliance and/or records retention purposes.

I understand that my e-mail and other electronically stored information may be subject to records retention requirements and/or disclosure, in accordance with applicable laws or as part of discovery proceedings in legal actions.

I further understand that any violation of the provisions of the District’s policy or regulations may result in disciplinary action as the District deems appropriate.

Employee Signature: _____ Date: _____