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, _LGS-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
1st Reading for Re-Adoption: September 29, 2020
2nd Reading and Re-Adoption: October 27, 2020