GREENBURGH ELEVEN USFD

POLICY #4526.2

ACCEPTABLE USE POLICY FOR TECHNOLOGY AND THE INTERNET

— SCHOOL DISTRICT EMPLOYEES —

The following Policy must be agreed to by the user before access will be provided to School District computer and Internet facilities. Use of such facilities after receipt of this Policy is deemed to constitute agreement.

Introduction

The School District furnishes computers, network facilities and equipment, and provides access to the Internet specifically to support learning and enhance instruction. The School District's intention is to promote educational excellence and to prepare students for an increasingly technological world. Hence, any use of the District's technological resources should facilitate enhanced research, innovation and communication.

The School District recognizes that with Internet access comes the potential for uses and the availability of material which are unrelated to scholarship. The District's computers, network and Internet facilities (including, without limitation, e-mail, discussion groups and Web-based tools) are to be used only in a manner consistent with the professional status of all District Employees and administrators and their responsibility as role models. Except for limited incidental (and in all instances, appropriate) use, employees should use their own computers and their own Internet access arrangements for personal purposes.

The responsibility for appropriate use of School District computers, network facilities and Internet access rests on the users themselves. The School District requires that anyone using its facilities act responsibly by reading, understanding and agreeing to the policies outlined below.

Everyone must understand that access to School District computers, network and Internet facilities is a revocable privilege, and not a right. Use of the system can and will be monitored by the School District, and there is no expectation of privacy in employee use.

Applicability and General Principles

These policies apply to anyone who uses School District computers, networked hardware, or who otherwise gains access to School District network facilities and/or the Internet via computer equipment and/or access lines located in the School District or elsewhere. This includes any remote access from off-site which involves the use of School District sites, servers, intranet facilities, e-mail accounts or software.

All users must make efficient, ethical and legal utilization of network resources. All users must be aware that material created, stored on, or transmitted from or via the system is not private. Internet use is inherently insecure. School District network administrators may review any and all individual computers and/or areas of the network at any time to ensure that the system is being used properly. For this reason, all users should expect that e-mails, materials placed on personal Web pages, and other work that is created on the network may be viewed by a third party.

Both internal and external network and Internet access will be provided to authorized users by the assignment of unique log-in identification codes ("usernames" and passwords) and, where appropriate, with limited hard disk space on School District hardware, for their own individual use. Authorized users will be personally responsible for maintaining the integrity of the School District's access policy, and may not permit other persons to use their usernames, passwords, accounts or disk space, or disclose their usernames, passwords or account information to any third party.

Usernames and passwords will be furnished subject to the provisions of this Policy, and such updates or modifications as may hereafter be promulgated.

Computer and network users must respect the integrity and security of the School District's systems and network, and the access privileges, privacy and reasonable preferences of other users. The School District reserves the right to limit access time and disk space in order to optimize an equitable allocation of resources among users.

The School District makes no warranties of any kind, whether express or implied, for the service it is providing. It is not responsible for any damages, including loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions, whether caused by the School District's negligence, or by a user's errors or omissions. Information obtained from the Internet is used at the user's own risk, and the School District specifically disclaims any responsibility for the accuracy or quality of information obtained by employees via access provided by or through the School District.

The following policies are intentionally broad in scope and, therefore, may include references to resources, technology and uses not yet available.

Rules of Conduct and Compliance

Anyone who violates this Acceptable Use Policy may have her/his access privileges suspended or revoked by the network administrator. In addition, further disciplinary action may be taken as permitted by applicable law and the terms of any applicable collective bargaining agreement.

Except as otherwise indicated below, all policies and prohibitions regarding users of the network also apply to users of individual School District computers.

1. The network may not be used to download, copy, or store any software, shareware, or freeware. This prohibition specifically includes copyrighted still, video and audio media files. Moreover, only an individual designated by the Superintendent or the Instructional Technology Coordinator is authorized to consent to the terms of any software license with respect to downloaded programs. This prohibition shall not apply to "fair use" of online media for teaching or scholarly purposes, as permitted by the United States copyright laws, where such use is strictly limited to a small excerpts from a work no greater than required for a permitted purpose; but in the case of any doubt, "fair use" questions should be referred to a network

administrator and/or the School District's legal counsel prior to any such downloading, uploading, copying or storage.

2. Computer and network users may not add (or attempt to add) any software, shareware, freeware or other applications to the School District's network or computers, or add to or modify any existing software or applications, without the express permission of the Superintendent or the Instructional Technology Coordinator. Any software which is installed must be properly acquired by the School District and licensed to the School District from the copyright owner thereof, and any modifications must comply with the terms of the applicable license(s). Software installation requests will not be implemented until required proof of School District ownership and license status has been reviewed and approved.

3. The School District's computers and network (including the use of such computers or the network to access the Internet) may not be used for any commercial purposes, and users may not offer or sell products or services through the system.

4. The School District's computers and network (including the use of such computers or the network to access the Internet) may not be used for advertising, political campaigning, or political lobbying.

5. The School District's computers and network (including the use of such computers or the network to access the Internet) may not be used for any activity, or to transmit any material, that violates United States, New York State or local laws. This includes, but is not limited to, fraudulent acts, violations of copyright laws, and any threat or act of intimidation or harassment against another person.

6. Our School District is a place of respect, responsibility, safety, tolerance and good manners. It is forbidden to use the network or any School District computer facilities for hate mail. Defamatory statements, statements intended to injure or humiliate others by disclosure of personal information (whether true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion are forbidden. Network users may not use vulgar, derogatory, or obscene language. Network users may not post anonymous messages or forge e-mail or other messages.

7. Computer and network users are strongly advised to use caution about revealing any information on the Internet, or storing such information on the School District's computers or the network, which would enable others to exploit them or their identities: this includes last names, home addresses, Social Security numbers, passwords, credit card numbers or financial institution account information, and photographs. Under no circumstances should a user reveal such information about another person without that person's express or prior consent.

8. Computer and network users may not log on to someone else's account, attempt to access another user's files, or permit anyone else to log on to their own accounts. Users may not try to gain unauthorized access ("hacking") to the files or computer systems of any other person or organization. However, employees must be aware that any information stored on or communicated through the School District network may be susceptible to "hacking" by a third party, and such information may be reviewed by the School District at any time, with or without prior notice.

9. Computer and network users may not access Web sites, newsgroups, or chat areas that contain material that is obscene or that promotes illegal acts. Likewise, use of the network to access,

process or store pornographic material (whether visual, auditory or written), or material which contains dangerous recipes, formulas or instructions, is prohibited.

10. The attention of all computer and network users is specifically directed to the School District's separate Internet Safety Policy, which applies to all users of School District computer and network facilities, and which is incorporated herein by reference. Any attempt to bypass, defeat or circumvent the Internet Safety Policy Technology Prevention Measures, which are designed to prevent access to visual depictions that are obscene, involve child pornography, or are harmful to minors is punishable as a violation of this Acceptable Use Policy. In addition, evidence of use of any computer or the network to access, store or disseminate child pornography will be referred to law enforcement authorities for investigation and prosecution as may be appropriate.

11. Computer and network users may not access chat rooms or social networking websites except for District business. While incidental personal use of e-mail facilities may be permitted, such incidental use will not be deemed a waiver of the School District's right to prohibit all such use, either on an individually-applicable or on a generally-applicable basis. Users understand and accept that no expectation of privacy attaches to any e-mail, including personal communications.

12. Computer and network users may not engage in "spamming" (sending irrelevant or inappropriate electronic communications individually or en masse) or participate in broadcast electronic communications (such as chain letters or other mass communications) other than for official School District purposes.

13. Computer and network users who maliciously access, alter, delete, damage or destroy any computer system, computer network, computer program, or data may be subject to criminal prosecution as well as to disciplinary action by the School District. This prohibition includes, but is not limited to, changing or deleting another user's account; changing the password of another user; using an unauthorized account; damaging any files; altering the system; using the system to make money illegally; destroying, modifying, vandalizing, defacing or abusing hardware, software, furniture or any School District property. Users may not develop programs that harass other users or infiltrate a computer or computer system and/or damage the software components of a computer or computer system (e.g., create viruses, worms) is prohibited.

14. Computer and network users may not intentionally disrupt information network traffic or crash the network and connected systems; they must not degrade or disrupt equipment or system performance. They must not download or save excessively large files without the express approval of the network administrator. Computer and network users may not add any software or applications to the School District's network or computers, or add to or modify any existing software or applications, without the express permission of the network administrator.

15. Computer and network users may not use such facilities to plagiarize, which is a serious academic offense. Plagiarism is "taking ideas or writings from another person and offering them as your own." Credit must always be given to the person who created the article or the idea. A person who, by cutting and pasting, or otherwise reproducing someone else's content, leads readers to believe that what they are reading is the person's original work when it is not, is guilty of plagiarism.

16. Computer and network users may not copy any copyrighted or licensed software from the Internet or from the network without the express permission of the copyright holder: software must be purchased or licensed before it can legally be used.

17. Computer and network users may not take data, equipment, software or supplies (paper, toner cartridges, disks, etc.) for their own personal use. Such taking will be treated as theft. Use of School District printers and paper must be reasonable.

18. The School District assumes no responsibility for student, faculty or staff websites created and hosted outside of the District network. Decisions to provide access to such external websites from the District network will be made on a case-by-case basis.

Violations and Consequences

Consequences of violations include but are not limited to:

- Suspension or revocation of information network access;
- Suspension or revocation of network privileges;
- Suspension or revocation of computer access;
- Disciplinary action, up to and including termination of employment;
- Criminal prosecution.

In addition, the School District may seek monetary compensation for damages in appropriate cases. Repeated or severe violations will result in more serious penalties than one-time or minor infractions.

This Acceptable Use Policy is subject to change. The School District reserves the right to restrict or terminate information network access at any time for any reason. The School District further reserves the right to monitor network activity as it sees fit in order to maintain the integrity of the network and to monitor acceptable use. School and District-wide administrators will make final determination as to what constitutes unacceptable use.

> Disciplinary penalties involving adverse employment action will be determined in accordance with applicable state law and the terms of applicable collective bargaining agreements. Final determination of penalties including the suspension or revocation of access privileges will be determined by the Superintendent of Schools or her/his designee.

Adopted: October 8, 2009
Readopted: July 9, 2015
Readopted: July 11, 2016
Readopted: July 13, 2017
Readopted: July 11, 2018