SUBJECT: ACCEPTABLE USE POLICY FOR ALL USERS OF THE DISTRICT COMPUTER NETWORK AND INTERNET SERVICES

The Bethpage Union Free School District appreciates the educational value of providing students and staff access to the District's Computer Network, including access to the Internet. Positive educational use of these resources has resulted in powerful learning experiences. The Board considers access to these resources to be an important educational research tool for students and staff in the 21st Century. However, access to the District's Computer Network and Internet is a privilege, not a right. As such, certain responsibilities fall upon the user to ensure proper use of these resources.

All users of the District's Computer Network and Internet must comply with this policy. Failure to comply may result in disciplinary action, as well as the suspension, restriction, and/or revocation of access privileges. For purposes of this policy, the term "Computer Network" shall refer to all of the District's computers, software, network capabilities, e-mail, Internet access and other technological supports.

Administration:

1. The Superintendent of Schools shall designate a Computer Coordinator to oversee the District's Computer Network.

2. The Computer Coordinator shall monitor and examine all Computer Network activities, as deemed appropriate, to ensure proper use of the system.

3. The Computer Coordinator shall ensure that District policy and rules governing use of the Computer Network is disseminated to all Computer Network users.

4. The Computer Coordinator shall provide employee training for proper use of the Computer Network and will ensure that staff who are responsible for supervising students in their use of the District's Computer Network, provide similar training to their students. In addition, the Computer Coordinator shall be responsible for ensuring that the District's policy and regulations regarding the use of the Computer Network, are reviewed with all Computer Network users, including students and staff.

5. The Computer Coordinator shall ensure that as part of the training provided, users are alerted to the privacy limitations placed on Computer Network users, as detailed herein.

6. The Computer Coordinator shall ensure that all disks and software loaded onto the Computer Network have been scanned for computer viruses. In this regard, the Computer Coordinator must approve all software or discs which are to be loaded onto the Computer Network, prior to their installation.

7. Building Principals shall ensure that parents/guardians are informed of the District's Acceptable Use Policy regarding the use of the Computer Network. Parents/guardians who object to their child's use of the District's Computer Network must notify their child's building principal, in writing, of their decision. The exclusion agreements shall be forwarded to and maintained by the Computer Coordinator, and those students whose parents/guardians have opted for them to be excluded, shall be unauthorized to use the District's Computer Network unless written consent is obtained from the student's parent/guardian, which indicates otherwise.

The Computer Coordinator shall be responsible for implementing reasonable precautions to

restrict a student's unauthorized use of the Computer Network. Students who gain unauthorized access to the Computer Network must abide by and are subject to discipline for violating the District's policies and regulations, including, but not limited to, the District's Student Discipline Code and the District's Computer Network Acceptable Use Policy. While the District shall institute reasonable precautions to restrict a student's unauthorized access to the Computer Network, the District is not responsible for any damages sustained or incurred in connection with a student's unauthorized access to the Computer Network.

Procedures for Proper Use

1. The District's Computer Network is provided to support the educational mission of the school. The use of the District's Computer Network must be consistent with the District's mission and goals.

2. Computer Network users must adhere to all of the District's policies and procedures including, but not limited to, the District's policies and regulations regarding student and employee conduct.

3. The individual in whose name an account is issued is responsible at all times for its proper use.

4. Computer Network users will be issued a log-in name and password. Passwords must be changed every 90 days.

5. Computer Network users identifying a security problem on the District's system must immediately notify an appropriate teacher, administrator, or the Computer Coordinator. Users should not demonstrate the problem to anyone.

6. Any Computer Network user who is identified as a security risk, or as having a history of violations of District computer use guidelines, may be denied access to the Computer Network.

7. Computer Network users have **NO EXPECTATION OF PRIVACY** with respect to any data stored or transmitted via the District's Computer Network, or used in conjunction with the Computer Network. School officials shall monitor the use of the District's Computer Network and can and will search, at any time, the account, e-mail, disks, files, or other data stored on the District's Computer Network.

Prohibitions

The following is a list of prohibited actions concerning use of the District's Computer Network. Violation of any of these prohibitions may result in discipline or other appropriate measure, including the suspension, restriction, and/or revocation of the user's access to the District's Computer Network.

1. All users are responsible for safeguarding their own passwords. Sharing of passwords without written permission from the teacher/administrator or Computer Coordinator, as appropriate, is prohibited. Users will be held accountable for the consequences of disclosing this information.

2. Attempts to read, delete, copy, or modify the electronic mail of other system users is prohibited as is any deliberate or reckless interference with the ability of their system users to

send/receive electronic mail. Forgery or attempted forgery of electronic mail messages is prohibited.

3. Students will not transmit personal information about themselves or others. This shall include pictures, addresses, phone numbers, pager numbers, and email addresses. All users shall take reasonable precautions to ensure against the disclosure of confidential information regarding students or others, when using the District's Computer Network.

4. No personal software or disks may be loaded onto the District's Computer Network without permission of the Computer Coordinator.

5. Attempts by a user to log on the District's system with the name of another individual, with or without the individual's password, is prohibited.

6. Use of the Computer for reasons other than educational purposes is prohibited.

7. Use of the Computer Network for commercial purposes is prohibited.

8. The Computer Network constitutes public facilities and may not be used to support or oppose political candidates or ballot measures.

9. Users are prohibited from using the Computer Network in connection with illegal activities and/or in any manner that is obscene, libelous, disruptive to school activities, or jeopardizes the health and safety of others. Transmission of material, information or software in violation of any District policy or regulation, local, state or federal law or regulation, is prohibited. Information pertaining to or implicating illegal or unlawful activity will be reported to the proper authorities.

10. Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available copyrighted software on the Computer Network is prohibited.

11. Vandalism will result in the severe restriction or cancellation of system privileges. Vandalism is defined as a malicious or reckless attempt to harm or destroy District equipment or materials, including software and related printed material, data of another user of the District's system or any of the agencies or other networks that are connected to the Internet. This includes, but is not limited to the uploading, downloading, or creating of computer viruses.

12. The use of the District's Computer Network in a manner that will disrupt the use of the District's technology for others, is also prohibited. Such abuse may include, but is not limited to, downloading extensive files, sending mass e-mail messages, or transmitting or propagating chain e-mail letters.