4321 ACCEPTABLE USE OF COMPUTER NETWORK(S)/ COMPUTERS AND RESOURCES BY SUPPORT STAFF MEMBERS

The school district provides computer equipment, computer services, and Internet access to its pupils and staff for educational purposes only. The purpose of providing technology resources is to improve learning and teaching through research, teacher training, collaboration, dissemination and the use of global communication resources. The "system administrators" referred to herein as employees of the school district who administer the school district computer network(s)/computers and the system administrators reserve the right to monitor all activity on network(s)/computer facilities/computers.

Because of the complex association between so many government agencies and computer network(s)/computers, support staff members must adhere to strict regulations. Regulations are provided here so that support staff members are aware of their responsibilities. The school district may modify these regulations at any time by publishing modified regulations on the network(s) and elsewhere.

Support staff members are responsible for good behavior on computer network(s)/computers. Communications on the computer network(s)/computers are often public in nature. Policies and Regulations governing support staff members behavior and communications apply. The school district's network(s), Internet access and computers are provided to conduct research and as a tool for instruction and to communicate with others. Access to computer network services/computers is given to support staff members who are expected to act in a considerate, responsible and professional manner. Access is a privilege, not a right. Access entails responsibility. Individual users of the district computer network(s)/computers are responsible for their behavior and communications over the computer network(s)/computers. It is presumed that users will comply with district standards. Beyond the clarification of such standards, the district is not responsible for the actions of individuals utilizing the computer network(s)/computers who violate the policies and regulations of the Board.

Computer network(s)/computer storage areas shall be treated in the same manner as other school storage facilities. Computer network(s)/computer administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. Users should not expect that files stored on district servers will always be private. Users should expect all files stored on district servers will be available for review by the Information Systems Manager and/or school administrators.

Within reasonable limits, freedom of speech and access to information will be honored.

Behaviors including but not limited to the following are prohibited:

1. Sending or displaying offensive messages or pictures;
2. Using obscene language;
3. Harassing, insulting or attacking others;
4. Damaging, degrading or disrupting computers, computer systems or computer network(s)/ computers;
5. Violating copyright laws;
6. Using another's password;
7. Trespassing in another's folders, work or files;
8. Intentionally wasting limited resources;
9. Employing the network(s)/computers for commercial purposes;
10. Engaging in other activities which do not advance the educational purposes for which computer network(s)/computers are provided;
11. Stealing data or other intellectual projects;
12. Forging electronic mail messages;
13. Posting anonymous messages;
14. Accessing school computers for other than educational purposes; and/or
15. Any other unethical, unacceptable, illegal and/or inappropriate activity.

Information Content and Uses of the System

Users agree not to publish on or over the system any information which violates or infringes upon the rights of any other person or any information which would be abusive, profane or sexually offensive to an average person, or which without the approval of the system administrators, contains any advertising or any solicitation of other members to use goods or services. The user agrees not to use the facilities and capabilities of the system to conduct any non-school related business or solicit the performance of any activity which is prohibited by law or is non-educational.

While most of the content available on the Internet is innocuous and much of it a valuable educational resource, some objectionable material exists. The Board will provide pupil access to Internet resources only in supervised environments and has taken steps to lock out objectionable areas to the extent possible, but potential dangers remain. Support staff members are advised that some systems may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal material and are to supervise pupil use of computers and the Internet. The Board and the system administrators do not condone the use of such materials and do not permit usage of such materials in the school environment. Support staff members should discipline pupils knowingly bringing such materials into the school environment in accordance with Board policies and regulations and inform pupils that such activities may result in termination of such pupils' accounts on the computer network(s) and their independent use of computers.

On-line Conduct

Any action by a support staff member or other user of the school district's computer network(s)/computers that is determined by a system administrator to constitute an inappropriate use of computer network(s)/computers resources or to improperly restrict or inhibit other members from using and enjoying those resources is strictly prohibited and may result in limitation on or termination of an offending member's account and other action in compliance with the Board policy and regulation. The user specifically agrees not to submit, publish, or display any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or otherwise illegal material; nor shall a user encourage the use, sale, or distribution of controlled substances. Transmission of material, information or software in violation of any local, state or federal law is also prohibited and is a breach of the Consent and Waiver Agreement.

Users agree to indemnify The Somerset Hills School District and the system administrators for any losses, costs, or damages, including reasonable attorneys' fees incurred by the Board relating to, or arising out of any breach of this section by the user.

Computer network(s)/computer resources are to be used by the user for his/her educational use only; commercial uses are strictly prohibited.

Software Libraries on the Network(s)

Software libraries on the network(s) are provided to support staff members as an educational resource. No support staff member may install, upload, or download software without the expressed consent of the system administrator. Any software having the purpose of damaging other members' accounts on the school district computer network(s)/computers (e.g., computer viruses) is specifically prohibited. The system administrators, at their sole discretion, reserve the rights to refuse posting of files and to remove files. The system administrators, at their sole discretion, further reserve the right to immediately limit usage or terminate the account or take other action consistent with the Board's policies and regulations of a member who misuses the software libraries.

Copyrighted Material

Copyrighted material must not be placed on any system connected to the network(s)/computers without the author's specific written permission. Only the owner(s) or persons they specifically authorize may upload copyrighted material to the system. Members may download copyrighted material for their own use in accordance with Policy and Regulation Nos. 2531, Copying Copyrighted Materials. Any member may also noncommercially redistribute a copyrighted program with the expressed written permission of the owner or authorized person. Permission must be specified in the document, on the system, or must be obtained directly from the author.

Public Posting Areas (Message Boards/Usenet Groups)

Usenet and Internet Relay Chat Room messages are posted from systems connected to the Internet around the world and the school district system administrators have no control of the content of messages posted from these other systems. To best utilize system resources, the system administrators will determine which Usenet groups are most applicable to the educational needs of the school district and will carry these groups on the school district computer network(s). The system administrators or the school

administration, at their sole discretion, may remove messages posted locally that are deemed to be unacceptable or in violation of the Board policies and regulations. The system administrators or the school administration, at their sole discretion, further reserve the right to immediately terminate the account of a member who misuses the message boards or Usenet groups.

Real-time, Interactive, Communication Areas

The system administrators, at their sole discretion, reserve the right to monitor and immediately limit the use of the computer network(s)/computers or terminate the account of a member who misuses real-time conference features (talk/chat/Internet relay chat) etc.

Electronic Mail

Electronic mail ("E-mail") is an electronic message sent by or to a member in correspondence with another person having Internet mail access. All messages sent and received on the school district computer network(s) must have an educational or administrative purpose and are subject to review. A sender of an E-mail message should expect the E-mail messages will be reviewed by the system administrators or the school administration. Messages received by the system are retained on the system until deleted by the recipient or for a maximum of thirty calendar days. A canceled account will not retain its E-mail. Members are expected to remove old messages within thirty calendar days or the system administrators may remove such messages. The system administrators may inspect the contents of E-mail sent by one member to an addressee, or disclose such contents to other than the sender or a recipient when required to do so by the Board policy, regulation or other laws and regulations of the State and Federal governments. The Board reserves the right to cooperate fully with local, state, or federal officials in any investigation concerning or relating to any E-mail transmitted on the school district computer network(s) or computers.

Disk Usage

The system administrators reserve the right to set quotas for disk usage on the system. A member who exceeds his/her quota of disk space will be advised to delete files to return to compliance with predetermined quotas. A member who remains in noncompliance of disk space quotas after seven school days of notification will have their files removed by a system administrator.

Security

Security on any computer system is a high priority, especially when the system involves many users. If a member feels that he/she can identify a security problem on the computer network(s), the member must notify a system administrator. The member should not inform individuals other than the system administrators or other designated members of the school district staff of a security problem. Professional staff may allow individuals who are not members to access the system through the staff personal account as long as the staff person does not disclose the password of the account to the individuals and understands that the staff person assumes responsibility for the actions of individuals using his/her account. Members may not otherwise allow others to use their account and password. Passwords to the system should not be easily guessable by others, nor should they be words which could be found in a dictionary. Attempts to log in to the system using either another member's account or as a system administrator will result in termination of the account. Members should immediately notify a system administrator if a password is lost or stolen, or if they have reason to believe that someone has obtained unauthorized access to their account. Any member identified as a security risk will have limitations placed on usage of the computer network(s)/computers or may be terminated as a user and be subject to other disciplinary action.

Vandalism

Vandalism will result in cancellation of system privileges and other disciplinary measures. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the system, or any of the agencies or other network(s)/computers that are connected to the Internet backbone or of doing intentional damage to hardware or software on the system. This includes, but is not limited to, the uploading or creation of computer viruses.

Printing

The printing facilities of the computer network(s)/computers should be used judiciously. Printing for other than educational, or school related purposes is prohibited.

Violations

Violations of the Acceptable Use of Computer Network(s)/Computers and Resources may result in a loss of access as well as other disciplinary or legal action. Disciplinary

action shall be taken as indicated in Policy and Regulation No. 4321, Support Staff Members, Acceptable Use of Computer Network(s)/Computers and Resources, Policy No. 4150, Support Staff Member Discipline, as well as possible legal action and reports to the legal authorities and entities.

Determination of Consequences for Violations

The particular consequences for violations of this policy shall be determined by the Information Systems Manager in matters relating to the use of computer network(s)/computers and by the Superintendent or designee in matters of discipline or employee suspension or actions by the authorities deemed to be the appropriate course of action.

Individuals violating this policy shall be subject to the consequences as indicated in Policy No. 2361 and other appropriate discipline which includes but are not limited to:

1. Use of Computer Network(s)/Computers only under direct supervision;
2. Suspension of network privileges;
3. Revocation of network privileges;
4. Suspension of computer privileges;
5. Revocation of computer privileges;
6. Suspension from employment;
7. Legal action and prosecution by the authorities.

Decisions of the Information Systems Manager may be appealed in accordance with the appropriate employee grievance procedure.

Issued: 1 October 2008