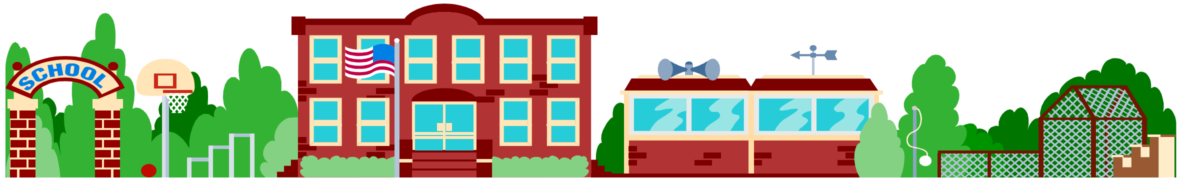
Appendix C: Policies

Revised July 2003

WEST ISLIP
COMPUTERIZED INFORMATION SERVICES
and WEBSITE POLICIES
for STAFF



The following network and Internet policies were created by a committee of teachers, administrators, paraprofessionals and parents and then, approved by the Board of Education. The intent of the policies is to protect the integrity of our network, insuring that each student, staff and community member has reasonable access to our network and the Internet. No policy is perfect, but through these policies we hope to convey the importance of our network to the daily operation of the District and the instruction of our students, and that disruptions to the system will not be tolerated.

It is extremely important that each district employee be familiar with the information contained within these policies. Once read, please sign the policy agreements found on the last page and return it to your building principal. Signed agreements will be kept on file in each building or at District Office.

Thank you for your help.

I. WORLD WIDE WEB: DISTRICT WEBSITES

POLICY

In order to support the vision and mission of the West Islip School District, the District will create and maintain_websites for the following purposes:

a) A place to showcase innovative student and staff educational projects, presentations and learning experiences.

b) A gateway to West Islip District and community resources and to educational websites.

c) A means for the community to access West Islip District information.

d) A means of "opening up" communications among students, West Islip District personnel, the community, and associated organizations.

The West Islip District websites may not be used for any unauthorized commercial and/or promotional activity.

Regulations will be developed for implementing guidelines as to staff/student access and usage of the West Islip District websites.

REGULATION

The availability of Internet access in the West Islip School District provides an opportunity for students and employees to contribute to West Islip's presence on the World Wide Web. The websites provide information to the world about curriculum, instruction, activities and information as enumerated in the West Islip District Web Policy.

The Director of Computer Education, building principals and district administrators will oversee and monitor the West Islip District websites for compliance with District policies, regulations and/or procedures. They must approve all webpages or links on the West Islip District websites.

All web authors must familiarize themselves with and adhere to the related West Islip District policies, regulations and procedures. Failure to follow these policies or regulations may result in the loss of authoring privileges or more stringent disciplinary measures in accordance with law and/or applicable collective bargaining agreement(s).

All West Islip District webpages must have an objective that conforms to the West Islip District Web Policy as well as West Islip District educational goals and objectives. Documents on the West Islip District's server or designated commercial server, as well as links to non-district servers, must reflect the standards for instructional resources/materials established in West Islip District policy and/or regulations. Webpages must also adhere to copyright laws.

Links to non-district servers (webpages) must contain a disclaimer indicating that the user is leaving a West Islip District website (server) and that the linked material is not regulated by the West Islip District. A sample disclaimer is listed below:

Disclaimer

> A great deal of thought and time has gone into choosing sites that are intended for student use. However, with the rapidly changing nature of websites and the World Wide Web, including the multitude of links located on each site, there is always the possibility that a student can access inappropriate material. For this reason, we stress the need for parental guidance and rules regarding the use of the Internet. At no time, should a student be using the Internet unsupervised.
>
> Please remember that the West Islip District has no control and assumes no responsibility for the ever-changing content of web sites linked to this site.

Webpages on the West Islip District's server or commercial servers paid for by West Islip are the property of the West Islip District. All webpages and the webserver will be examined periodically to check for the timeliness and relevance of its pages.

Student Safeguards

Webpages may include, but are not required to include, the first name and the initial of the student's last name. Pages or filenames may not include a student's telephone number, address, e-mail address, or names of other family members or friends.

No student under the age of eighteen (18) years of age shall be personally identified in a picture or video on a West Islip District webpage without a signed parent/guardian approval on file with the appropriate administrator. Parents may request their child’s name and/or picture be excluded from a webpage through submission of a letter to the building principal.

Employee Safeguards

No personal information about employees except name and building may be published. Employees may request that their picture be excluded from a webpage through submission of a letter to the building principal/district coordinator.

II. STAFF USE OF COMPUTERIZED INFORMATION RESOURCES

Personnel

The West Islip District's computer information system (consisting of software, hardware, electronic communications lines and devices, servers, terminals, printers, CD-ROM devices, tape drives, mainframe and personal computers. - DIS hereafter) is provided for staff to enhance the educational programs of the West Islip District, to further District goals and objectives; and to conduct research and provide information; and to communicate with others.

Generally, the same standards of acceptable staff conduct, which apply to any aspect of job performance, shall apply to use of the DIS. The standards of acceptable use as well as prohibited conduct by staff accessing the DIS, as outlined in West Islip District policy and regulation, are not intended to be all-inclusive. The staff member who commits an act of misconduct which is not specifically addressed in West Islip District policy and/or regulation may also be subject to disciplinary action, including loss of access to the DIS as well as the imposition of discipline under the law and/or the applicable collective bargaining agreement. Legal action may also be initiated against a staff member who willfully, maliciously or unlawfully damages or destroys property of the District.

Staff are encouraged to utilize electronic communications in their roles as employees of the West Islip District- Staff are also encouraged to utilize electronic means to exchange communications with parents/guardians or homebound students, subject to appropriate consideration for student privacy. Such usage shall be limited to school related issues or activities. Communications over the DIS are often public in nature; therefore, general rules and standards for professional behavior and communications will apply.

The West Islip District's policies and accompanying regulations for staff and student use of computerized information resources, establish guidelines for staff to follow when instructing and working with students on acceptable student use of the DIS, including access to external computer networks.

Privacy Rights

Staff data files, E-mail and electronic storage areas shall remain West Islip District property, subject to West Islip District control and inspection. The computer coordinator may access all such files and communications to insure system integrity and that users are complying with requirements of West Islip District policy and accompanying regulations. Staff should NOT expect that information stored on the DIS will be private.

Prohibitions

It is not the intention of this regulation to define all inappropriate usage. However, in addition to the general requirements of acceptable staff behavior, activities that shall be prohibited by staff members using the DIS include, but are not limited to the following:

1. Using the DIS in any way that results in unauthorized charges or expense to the West Islip District.

2. Damaging, disabling or otherwise interfering with the operation of computers, computer systems, software or related equipment through physical action or by electronic means.

3. Using unauthorized software on the DIS.

4. Changing, copying, renaming, deleting, reading or otherwise accessing files or software not created by the staff member without expressed permission from the computer coordinator.

5. Violating copyright law.

6. Employing the DIS for commercial purposes, product advertisement or political lobbying.

7. Disclosing an individual password to others or using others' passwords.

8. Sharing confidential information about students and/or employees.

9. Sending or displaying offensive messages or pictures.

10. Using obscene language.

11. Harassing, insulting or attacking others.

12. Engaging in practices that threaten the DIS (e.g., loading files that may introduce a virus).

13. Violating regulations prescribed by the network provider.

14. Use of the DIS for other than school related work or activities.

15. Assisting a student to violate West Islip District policy and/or regulation, or failing to report knowledge of any student violations of the West Islip District's policy and regulation on student use of computerized information resources.

16. Use which violates any other aspect of West Islip School District policy and/or regulations, as well as local, state or federal laws of regulations.

17. Compromising the DIS's limitations such as band width and disk space. (For example, storing a high volume of digital pictures and graphics, video conferencing and streaming video or audio.)

18. Any user of the DIS that accesses another network or other computer resources shall be subject to that network's acceptable use policy.

SANCTIONS

Any identified inappropriate behavior will be reported to the staff member's supervisor who will take appropriate disciplinary action. Any other violations or complaints will be routed to the staff member's supervisor for appropriate action. Violations may result in a loss of access to the DIS and/or disciplinary action. When applicable, law enforcement agencies may be involved.

NOTIFICATION

All staff will be given a copy of the West Islip District's policies on staff and student use of computerized information resources and the regulations established in connection with those policies. Each staff member will sign an acceptable use agreement before establishing an account or continuing his or her use of the DIS.

WEST ISLIP
INTERNET POLICIES
For STAFF

This Internet usage policy is designed to help you understand our expectations for the use of the Internet, and to help you use the District's resources wisely. All existing District policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of District resources, sexual harassment, information and data security, and confidentiality. While our direct connection to the Internet offers a multitude of potential benefits, it can also open the door to some significant risks to our data and systems if we do not follow appropriate security discipline. An Internet user can be held accountable for any breach of security or confidentiality resulting from their use of the District's Internet connection

INTERNET USAGE POLICY

This Internet Usage Policy applies to all individuals using the District system – including, but not limited to employees, students and community members. The entire Internet Usage Policy is attached to this document. Please read the policy and return the Acknowledgment to your principal.

Certain terms in this policy should be understood expansively to include related concepts. "District" includes all buildings and individuals. "Document" covers any kind of file that can be read on a computer screen as if it were a printed page, including HTML files read in an Internet browser, any file meant to be accessed by a word processing or desktop publishing program or its viewer, or the files prepared for the Adobe Acrobat reader and other electronic publishing tools. "Graphics" includes photographs, pictures, animations, movies, or drawings. "Display" includes monitors, flat-panel active or passive matrix displays, monochrome LCD's, projectors, televisions and virtual-reality tools.

Overview

This District provides access to the vast information resources of the Internet to help you do your job and be well informed. The facilities that provide access represent a considerable commitment of resources for telecommunications, networking, software, storage, etc. This Internet usage policy is designed to help you understand our expectations for the use of Internet resources, and to help you use those resources wisely.

While we have set forth-explicit requirements for Internet usage below, we would like to start by describing our Internet usage philosophy. **First and foremost, the Internet for this District is an educational tool, provided to you at significant cost. That means we expect you to use your Internet access primarily for educational-related purposes, i.e., to communicate with parents, students and teachers, to research relevant topics and obtain useful educational information (except as outlined in the following pages).** We insist that you conduct yourself honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as you would in any other educational dealings. To be absolutely clear on this point, all existing District policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of District resources, sexual harassment, information and data security, and confidentiality.

Unnecessary or unauthorized Internet usage causes network and server congestion. It slows other users, takes away from work time, consumes supplies, and ties up printers and other shared resources. Unlawful Internet usage may also garner negative publicity for the District and expose the District to significant legal liabilities.

Chats, newsgroups and e-mail give each individual Internet user an immense and unprecedented reach to promote a positive District image and tell our educational story. Because of that power, we must take special care to maintain the clarity, consistency and integrity of the District's educational image and posture. Anything any one individual writes in the course of acting for the District on the Internet could be taken as representing the District's educational posture. That is why we expect you to forego a measure of your individual freedom when you participate in chats or newsgroups on District time, as outlined below.

While our District connection to the Internet offers a multitude of potential benefits, it can also open the door to some significant risks to our data and systems if we do not follow appropriate security discipline. As presented in greater detail below, that may mean preventing machines with sensitive data or applications from connecting to the Internet entirely, or it may mean that certain users must be prevented from using certain Internet features like file transfers. The overriding principle is that security is to be everyone's first concern. District individuals can be held accountable for any breach of security or confidentiality.

INTERNET POLICY PROVISIONS

A) General

1. The District has software and systems in place that monitor, tract and record all Internet usage. Our security systems are capable of recording (for each and every user) each World Wide Web site visit, each chat, newsgroup or e-mail message, and each file transfer into and out of our internal networks, and we reserve the right to do so at any time. No individual should have any expectation of privacy as to his or her Internet usage. District officials will review Internet activity and analyze usage patterns, and they may choose to publicize this data to assure that District Internet resources are devoted to maintaining the highest levels of productivity.

2. We reserve the right to inspect all files stored in private areas of our network in order to assure compliance with policy.

3. The display of any kind of sexually explicit image or document on any District system is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.

The District uses independently supplied software and data to identify inappropriate or sexually explicit Internet sites. We may block access from within our networks to all such sites that we know of. If you find yourself connected accidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program.

4. This District's Internet facilities and computing resources must not be used to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction in any material way. Use of any District resources for illegal activity is grounds for immediate dismissal, and we will cooperate with any legitimate law enforcement activity.

5. Any software or files downloaded via the Internet into the District network become the property of the District. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

6. No individual may use District facilities to download or distribute pirated software or data.

7. No individual may use the District's Internet facilities to create or propagate any virus, worm, Trojan horse, or trap-door program code.

No individual may use the District’s Internet facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.

8. Each individual using the Internet facilities of the District shall identify himself or herself honestly, accurately and completely (including one's District affiliation and function where requested) when participating in chats or newsgroups, or when setting up accounts on outside computer systems.

9. Only those individuals or officials who are authorized to speak to the media, to analysts or at public gatherings on behalf of the District may speak/write in the name of the District to any newsgroup or chat room. While individuals may participate in newsgroups, e-mail or chats in the course of the school day when relevant to their duties, they do so as individuals speaking only for themselves.

Where an individual is identified as an agent of the District, the individual must refrain from any political advocacy and the unauthorized endorsement or appearance of endorsement by the District or its affiliates of any commercial product or service. Only those administrators and District officials who are authorized to speak to the media, to analysts or in public gatherings on behalf of the District may grant such authority to newsgroups or chat room participants.

10. The District retains the copyright to any material posted to any forum, newsgroup, chat or World Wide Web page by any individual in the course of his or her duties.

11. Individuals are reminded that chats and newsgroups are public forums where it is inappropriate to reveal confidential District information, student or individual data and any other material covered by existing District privacy policies and procedures. Individuals releasing such confidential information via a newsgroup, e-mail or chat - whether or not the release is inadvertent - will be subject to the penalties provided in existing District policies and procedures.

12. Use of District Internet access facilities to commit infractions such as misuse of District assets or resources, sexual harassment, unauthorized public speaking and misappropriation of intellectual property are also prohibited by general District policy and will be sanctioned under Board policies.

13. A wide variety of materials may be considered offensive by colleagues, parents or students, therefore, it is a violation of District policy to store, view, print or redistribute any document or graphic file that is not directly related to the user’s job or the District’s educational activities.

14. Individuals may use their Internet facilities for non-educational research or browsing during mealtime or other breaks, or outside of work hours, if all other usage policies are adhered to.

15. Individuals with Internet access must take particular care to understand the copyright, trademark, libel, slander and public speech control laws, so that our use of the Internet does not inadvertently violate any laws which might be enforceable against us.

16. Only Individuals with prior approval may download software for direct educational use, and must arrange to have such software properly licensed and registered as indicated in software licensing agreement. Downloaded software must be used only under the terms of its license.

17. No individual may use District Internet facilities to play or download games or entertainment software.

18. No individual may upload any software licensed to the District or data owned or licensed by the District without the express authorization of the administrator responsible for the software or data.

B) Technical

1. Continuous stock tickers, weather reports, streaming audio or video, etc., are strictly prohibited.

2. Individuals should schedule communications-intensive operations such as large file transfers, video downloads, mass e-mailings and the like for off-peak times.

3. Any file that is downloaded must be scanned for viruses before it is run or accessed.

C) Security

1. User ID's and passwords help maintain individual accountability for Internet resource usage. Any individual who obtains a password must keep that password confidential. District policy prohibits the sharing of user ID's or passwords.

2. The District has installed an Internet firewall to assure the safety and security of the District's Networks. Any individual who attempts to disable, defeat or circumvent any District security facility will be subject to disciplinary actions.

3. Files containing sensitive District data, as defined by existing Board security policy, that are transferred in any way across the Internet, must be encrypted.

4. Only those Internet services and functions without documented educational purposes for this District may not be enabled at the Internet firewall.

Summary of Internet Policy Provisions

1. The District has software and systems in place that can monitor and record all Internet usage.

2. The District reserves the right to inspect all files stored in private areas of our network in order to assure compliance with policy.

3. Sexually explicit material may not be displayed, archived, stored, distributed, edited or recorded using the District's network or computing resources.

4. Use of any District resources for illegal activity will be reported to the proper authorities and the appropriate disciplinary action will be taken against the individual(s). If necessary, the District will cooperate with all law enforcement agencies.

5. Any software or files downloaded via the Internet into the District network become the property of the District. Any material posted to any forum, newsgroup, chat or World Wide Web page according to copyrights or licenses.

6. No individual may use District facilities to knowingly download or distribute pirated software or data.

7. No individual may use the District's Internet facilities to create or deliberately propagate any virus, worm, Trojan horse, or trap-door program code. Also, to disable or overload any computer system or network.

8. Each individual using the Internet facilities of the District shall identify himself or herself honestly, accurately and completely (including one's District affiliation and function where requested) when participating in chats or newsgroups, or when setting up accounts on outside computer systems.

9. Only those individuals who are duly authorized to speak to the media, to analysts or in public gatherings on behalf of the District may speak/write in the name of the District to any newsgroup, e-mail or chat room.

10. The District retains the copyright to any material posted to any forum, newsgroup, chat or World Wide Web page by any individual.

11. Individuals releasing protected information by any means, whether or not the release is inadvertent, will be subject to all penalties under existing data security policies and procedures.

12. Use of District Internet access facilities to commit infractions such as misuse of District assets or resources, sexual harassment, unauthorized public speaking and misappropriation of intellectual property are also prohibited by general District policy and will be sanctioned under Board policies.

13. A variety of materials may be considered offensive by colleagues, parents, or students. Therefore, it is a violation of District policy to store, view, print or redistribute any document or graphic file that is not related to the user's job or the District's educational activity.

14. Individuals may use their Internet facilities for non-educational research or browsing during mealtime or other breaks, or outside of work hours, provided all usage policies are adhered to.

15. Individuals with Internet access must take particular care to practice copyright, trademark, and libel, slander and public speech control laws.

16. Only individuals with prior approval may download software, which may only be used under the terms of its license. Individuals are prohibited from using continuous downloads (such has continuous news and weather broadcasts, stock market ticker, music, video, images, etc.).

17. No individual may use District Internet facilities to play or download entertainment software or games.

18. No individual may upload any software licensed to or by the District or data owned or licensed to the District. Unauthorized transfer of data over the Internet is prohibited.

WEST ISLIP STAFF AGREEMENT FOR THE USE OF COMPUTERIZED INFORMATION RESOURCES AND THE INTERNET

In consideration for the privilege of using the West Islip District's Computer Information System (DIS), I agree that I have been provided with a copy of the West Islip District's policies on staff and student use of computerized information resources and the regulations established in connection with those policies. I agree to adhere to the staff policy and regulations and to any changes or additions later adopted by the West Islip District. I also agree to adhere to related policies published in any staff handbooks. I shall report all violations of the West Islip District's policy on use of computerized information resources to District officials.

____

INITIAL

I understand that failure to comply with these policies and accompanying regulations may result in the loss of my access to the West Islip District's Computer Information System (DIS) on the Internet and may, in addition, result in the imposition of discipline under the law and/or the applicable collective bargaining agreement. I further understand that the West Islip District reserves the right to pursue disciplinary action against me if I willfully, maliciously or unlawfully damage or destroy property of the West Islip District.

____

INITIAL

____

Staff Member Signature

____

Date

____

School/Building