WNYRIC INTERNET ACCESS AND SECURITY PROCEDURES AGREEMENT FORM

a) The Board of Education of the _____(Institution Name) has adopted policies that address the following:
   1. Staff Use of Computerized Information Resources
   2. Student Use of Computerized Information Resources
   3. The Children's Internet Protection Act (CIPA): Internet Content Filtering/Safety

b) Any actions by an individual user deemed unacceptable or a breach of the _____ (Institution Name) Acceptable Use Policy shall be subject to review and discipline by the institution. It is the institution's decision to determine and implement any necessary action to limit or terminate individual user access to the WNYRIC Internet service.

c) Inappropriate use of the system which improperly restricts or inhibits other users from accessing the network is strictly prohibited. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer viruses and/or unauthorized entry into any other system on the network.

d) The Western New York Regional Information Center is not responsible for inappropriate information or content found on the Internet.

e) The Western New York Regional Information Center is not liable for any damages or costs incurred as the result of individual use of the WNYRIC Internet service.

f) The Western New York Regional Information Center retains the final authority on the delivery of Internet service to the institution.

g) The Internet access is intended for the sole use of the individual users of the institution. Any use outside Institutional Use is prohibited without the expressed written consent of the WNYRIC.

h) This agreement will be reviewed and updated annually, to reflect new technology and any Internet Service Provider changes or requirements directed to WNYRIC as the service provider to school districts. This will include communication to participating school districts of any additions or changes, as well as documented approval by the school superintendent.

****

Institution: _____

Superintendent: (Print) _____

Superintendent: (Signature) _____ Date: _____

WNYRIC Chief Information Officer: (Print) _____

WNYRIC Chief Information Officer: (Signature) _____ Date: _____

WNYRIC INTERNET ACCESS AND SECURITY AGREEMENT

Erie 1 BOCES is a Board of Cooperative Educational Services located within Erie County. The Western New York Regional Information Center, ("WNYRIC" hereafter) is an institution within the Erie 1 BOCES which offers services to school districts, and other public agencies, many of which are not component districts of Erie 1 BOCES. The WNYRIC offers educational resources including the provision of Internet access. The WNYRIC Advisory Council consists of local BOCES and component district representatives who advise the Erie 1 BOCES Board, the District Superintendent and the Chief Information Officer for the RIC/Technology Services on matters concerning the operation of the WNYRIC. The Erie 1 BOCES Board believes that a written procedure that defines the limits of permissible use of the system by institutions and individuals together with sanctions for inappropriate use will help in developing, maintaining and operating this shared Internet connection.

The Internet

The WNYRIC provides an Internet service that best promotes teaching, learning and educational management across all its constituencies. This procedure defines acceptable use and security of the WNYRIC Internet Service by institutional and individual users.

Purposes

The purposes of this procedure are:

a) To define the users of the WNYRIC Internet service.

b) To define the acceptable use of the WNYRIC Internet service.

c) To identify procedures to address allegations of inappropriate use and to establish sanctions for such use.

d) To provide a WNYRIC Internet Access and Security Procedures Agreement form to be signed and periodically reviewed by the Chief School Officer or designated official of the institutional user and returned to the WNYRIC.

e) To aid the institutional users of the WNYRIC Internet service connection in developing and implementing their own policies which conform to this regional procedures document.

Users of the WNYRIC Internet Service

Institutional Users

Institutional users are organizations obtaining Internet access through the WNYRIC including: school districts, BOCES, and any community organization or public agency that is authorized to utilize the WNYRIC as their Internet service provider.

Individual Users

Individual users are defined as employees or students of an institutional user, or an appropriately authorized person affiliated with a community organization or public agency that is authorized to utilize the WNYRIC as their Internet service provider and who are provided with Internet access.

Acceptable Use of the WNYRIC Internet Service

Institutional Users

a) All institutional users of the WNYRIC Internet access must have written policies, adopted by the institution's Board of Education or other governing body, which specify that Internet access is being provided for educational purposes. The policies should restrict individual use to educational purposes. Further, the institution's Acceptable Use Agreement (AUP), as well as other Institutional policies, must address the following issues, which pertain to individual users:

   1. unacceptable standards of behavior
   2. the unlawful use of copyrighted materials
   3. illegal and commercial uses of the Internet
   4. access of inappropriate information
   5. failure to adhere to CIPA regulations
   6. use for work or activity that is inconsistent with the educational purpose of the Institutional User provided Internet service
   7. use of unauthorized software
   8. unauthorized access to files
   9. failure to adhere to required security procedures

b) Institutional users shall develop, implement and maintain security procedures to insure the integrity of authorized confidential materials obtained through the WNYRIC Internet service.

c) Institutional user agreements shall provide that the Institution will retain ownership of individual user data files, all of which shall be subject to institutional control and inspection.

d) Institutional user agreements shall require individual users to abide by the requirements, responsibilities and expectations established in the Institution's Acceptable Use Agreement.

e) Institutional user agreements shall establish procedures to address violations of the institution's or the WNYRIC's Acceptable Use Procedures by individual users. The agreement shall provide that an individual user's access to the Internet through the WNYRIC shall be limited, suspended or terminated by the Institution if it is determined that an individual user has violated the Acceptable Use Agreement. The Agreement shall also provide for notice to the individual user (and to his/her parents if the individual user is a student) of the alleged violation of the Acceptable Use Agreement. The individual user shall be provided with an opportunity to respond to such allegations. Any restriction or termination of individual access shall be the responsibility of the Institutional User.

f) The Internet access is intended for the sole use of the individual users of the institution. Any use outside Institutional Use is prohibited without the expressed written consent of the WNYRIC. It is a violation of law to provide (free or with fees) Internet access and services to private entities or private individuals of communities through the Institution.

Individual Users

All individual users must abide by the requirements, responsibilities and expectations established in the Institution's Acceptable Use Agreement. The individual users' Internet access is conditioned upon adherence to the requirements of that Agreement.

Network Security

Each school district/agency is responsible for the security of its own internal networks, equipment and hardware, software and software applications. WNYRIC assumes no responsibility or liability for failures or breach of district/agencies protective measures, whether implied or actual. Abuse that occurs as a result of the school district's systems or account being compromised may result in suspension of Internet access by WNYRIC for a period of time to assess the situation. If a security-related problem is escalated to WNYRIC for resolution, WNYRIC will resolve the problem in accordance with its current procedures. Generally, the following activities are prohibited: fraudulent, deceptive or misleading activities of any kind; network disruptions of any kind, including excessively burdensome uses that may impact network operation; or any unauthorized access, exploitation, interception or monitoring.

WNYRIC reserves the right to suspend Internet access for school district's failure to comply with any material requirements of our WNYRIC procedures, which suspension may be immediate and may have a fixed or indefinite duration.

Responsibilities and Procedures

This Acceptable Use and Security Procedure for WNYRIC Internet Access details the responsibilities of institutional and individual users regarding the utilization of the WNYRIC Internet services. The following subsections outline the processes that will take place should an institution or an individual fail to use the service in a responsible manner.

a) When an Institution fails to meet its responsibilities as outlined herein.

   The intent of this document is to outline acceptable uses of the Internet in order to minimize or avoid violations of agreed-upon procedures. However, serious or repeated failure to meet the agreed-upon responsibilities by the institutional user shall result in a referral to the WNYRIC Advisory Council for review and a recommendation to the Erie 1 BOCES District Superintendent. The (institutional) user shall be provided with notice of alleged violations of this procedure and shall have an opportunity to respond to the alleged violations before the WNYRIC Advisory Council prior to any recommendation to the District Superintendent. Recommended actions may include suspension, limitation or cancellation of the institution's Internet access through the WNYRIC. The decision of the District Superintendent may be appealed to the Erie I BOCES Board. The decision of the Board shall be final.

b) When an individual fails to meet his/her responsibilities as outlined herein.

   Institutional users shall determine, pursuant to procedures established in their acceptable use policies, codes of conduct, and/or collective bargaining agreements, if an individual user's access to the Internet through the WNYRIC shall be limited, suspended or terminated. The Institutional user is responsible for all concerns brought to their attention regarding their individual users. The WNYRIC shall have no responsibility for limitation of individual access. The Institution shall determine if any further disciplinary actions are necessary.

Appendix A

CHILDREN'S INTERNET PROTECTION ACT (CIPA)

Background

The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress in December 2000 to address concerns about access in schools and libraries to the Internet and other information. For any school or library that receives discounts for Internet access or for internal connections, CIPA imposes certain requirements. In early 2001, the Federal Communications Commission (FCC) issued rules to ensure that CIPA is carried out.

What CIPA Requires

a) Under CIPA, schools and libraries subject to CIPA do not receive the discounts offered by the "E-Rate" program (discounts that make access to the Internet affordable to schools and libraries) unless they certify that they have certain Internet safety measures in place. These include measures to block or filter pictures that: (a) are obscene, (b) contain child pornography, or (c) when computers with Internet access are used by minors, are harmful to minors;

b) Schools subject to CIPA are required to adopt a policy to monitor online activities of minors; and

c) Schools and libraries subject to CIPA are required to adopt a policy addressing: (a) access by minors to inappropriate matter on the Internet and World Wide Web; (b) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and (e) restricting minors' access to materials harmful to them. CIPA does not require the tracking of Internet use by minors or adults.

For the school year July 2001 through June 2002 and thereafter, schools and libraries were required to certify that they had their safety policies and technology in place, or that they were taking the necessary actions to put them in place before receiving E-rate funding for the following school year.

After a lower court found the application of CIPA to libraries unconstitutional, the United States Supreme Court upheld the statute in *U.S. v. American Library Association*.

Go to this web site for more details: http://www.fcc.gov/cgb/consumerfacts/cipa.html

STUDENT USE OF COMPUTERS IN THE SCHOOL DISTRICT (NCLB)

The Enhancing Education through Technology Act of 2001 is part of No Child Left Behind legislation. The goals are:

a) To improve student academic achievement through the use of technology in elementary schools and secondary schools.

b) To assist every student in crossing the digital divide by ensuring that every student is technologically literate by the time the student finishes the eighth grade, regardless of the student's race, ethnicity, gender, family income, geographic location, or disability.

c) To encourage the effective integration of technology resources and systems with teacher training and curriculum development to establish research-based instructional methods that can be widely implemented as best practices by State educational agencies and local educational agencies.

In an effort to inform parents about the use of computers in your school district, you may choose to ask the parent/guardian of each student to sign a written consent form. If you prefer, you may choose to inform the parent/guardian of the program and ask only that the parent/guardian inform you of any objection to the use of computers in the school. **An objection to this part of the curriculum may only be based on specific materials relating to health and hygiene if these materials are in conflict with the religion of the parent/guardian.**

A sample of each type of form is included in Appendix B. Also included is a form that a student may sign to acknowledge the receipt of school rules for computer use. Since a student is a minor, this form is advisory only.

School districts are also encouraged to incorporate violations and consequences of misuse or misbehavior involving computers into the school district's Code of Conduct.

APPENDIX B - SAMPLE POLICIES/FORMS

The following documents provide sample language for policies along with agreements for staff and students that may be used in whole or in part by your school district. The language should be carefully reviewed. Determination of what really fits your school district's technology environment will dictate what portions of the agreements are used in your employee computer use agreements.

a) Staff Use of Computerized Information Resources (sample BOE policy)

b) Erie 1 BOCES - Employee Computer Use Agreement

c) Student Use of Computerized Information Resources - Acceptable Use Policy (sample BOE policy)

d) Agreement for Student Use of Computerized Information Resources

e) Parental/Guardian Consent for Student Use of District Computerized Information Resources

f) Student and Parent Agreement

g) The Children's Internet Protection Act: Internet Content Filtering/Safety Policy (sample BOE policy)

If you would like to have these sample documents sent to you electronically, please contact Cinda West, Erie 1 BOCES Policy Services, at 716-821-7072 or cwest@e1b.org.

Personnel

SUBJECT:STAFF USE OF COMPUTERIZED INFORMATION RESOURCES

The Board of Education will provide staff with access to various computerized information resources through the District's computer system (DCS hereafter) consisting of software, hardware, computer networks and electronic communication systems. This may include access to electronic mail, so-called "on-line services" and the "Internet." It may also include the opportunity for some staff to have independent access to the DCS from their home or other remote locations. All use of the DCS, including independent use off school premises, shall be subject to this policy and accompanying regulations.

The Board encourages staff to make use of the DCS to explore educational topics, conduct research and contact others in the educational world. The Board anticipates that staff access to various computerized information resources will both expedite and enhance the performance of tasks associated with their positions and assignments. Toward that end, the Board directs the Superintendent or his/her designee(s) to provide staff with training in the proper and effective use of the DCS.

Staff use of the DCS is conditioned upon written agreement by the staff member that use of the DCS will conform to the requirements of this policy and any regulations adopted to ensure acceptable use of the DCS. All such agreements shall be kept on file in the District office.

Generally, the same standards of acceptable staff conduct which apply to any aspect of job performance shall apply to use of the DCS. Employees are expected to communicate in a professional manner consistent with applicable District policies and regulations governing the behavior of school staff. Electronic mail and telecommunications are not to be utilized to share confidential information about students or other employees.

This policy does not attempt to articulate all required and/or acceptable uses of the DCS; nor is it the intention of this policy to define all inappropriate usage. Administrative regulations will further define general guidelines of appropriate staff conduct and use as well as proscribed behavior.

District staff shall also adhere to the laws, policies and rules governing computers including, but not limited to, copyright laws, rights of software publishers, license agreements, and rights of privacy created by federal and state law.

Staff members who engage in unacceptable use may lose access to the DCS and may be subject to further discipline under the law and in accordance with applicable collective bargaining agreements. Legal action may be initiated against a staff member who willfully, maliciously or unlawfully damages or destroys property of the District.

Privacy Rights

Staff data files and electronic storage areas shall remain District property, subject to District control and inspection. The computer coordinator may access all such files and communications to

(Continued)

SUBJECT: STAFF USE OF COMPUTERIZED INFORMATION RESOURCES (Cont'd.)

ensure system integrity and that users are complying with requirements of this policy and accompanying regulations. Staff should **NOT** expect that information stored on the DCS will be private.

Implementation

Administrative regulations will be developed to implement the terms of this policy, addressing general parameters of acceptable staff conduct as well as prohibited activities so as to provide appropriate guidelines for employee use of the DCS.

NOTE: Refer also to Policy #8000 -- The Children's Internet Protection Act: Internet Content Filtering/Safety Policy

Adoption Date

SAMPLE FORM

Erie 1 BOCES -- Employee Computer Use Agreement

Every Erie 1 BOCES employee will be required to sign this computer Acceptable Use Agreement. This form supersedes previous forms. Employees who have signed previous forms must also complete this new form.

Computer use is often a valuable and necessary component of an employee's work. In addition, varying work responsibilities result in access to information sources such as software, programs, the Internet, and the district's computer network. Although employees may have access to these information sources, their use must be specially authorized. Access and authorization to information and equipment carry a corresponding responsibility to their appropriate use. Access should be primarily for educational and professional or career development activities. All hardware, including computers and equipment, is the property of Erie 1 BOCES and will fall under the guidelines listed below. Expectations of employees include, but are not limited to, the following:

a) Student Personal Safety
   1. Employees who supervise students with access to technical resources shall be familiar with the Erie 1 BOCES Student Internet Use Agreement and enforce its provisions.
   2. All student computer use must be supervised.

b) Illegal or Destructive Activities
   1. Employees shall not go beyond their authorized access to the district network or other computer equipment or software including the files or accounts of others.
   2. Employees shall not disrupt or attempt to damage or disrupt any computer, system, system performance, or data.
   3. Employees shall not use district equipment to engage in illegal acts.

c) System Security
   1. Employees are responsible for the security of their computer equipment, files and passwords.
   2. Employees shall promptly notify their immediate supervisor of security problems.
   3. Employees with access to student records may not use, release, or share these records except as authorized by Federal and State law.

d) Inappropriate Conduct
   The following are prohibited when using any technical resource:
   1. Obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language;
   2. Potentially damaging, dangerous, or disruptive material;
   3. Personal or generalized harassment in violation of district policies; and
   4. False or defamatory information.

e) Plagiarism and Copyright Infringement
   1. Works may not be plagiarized.
   2. The rights of copyright owners are to be respected. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by copyright. If an employee is unsure whether or not a work can be used, the copyright owner should be contacted for permission.
   3. Software copyrights and software licenses must be strictly respected.

(Continued)

Erie 1 BOCES -- Employee Computer Use Agreement (Cont'd.)

f) Inappropriate Access to Material
   1. Technical resources shall not be used with material that is profane, obscene (pornographic), or advocates illegal acts, violence, or illegal discrimination.
   2. Business use of instant messaging within Lotus Notes is allowed for Erie 1 staff. Personal messages are not permitted. The use of Internet games, web chats, unauthorized software, or other instant messaging software (e.g. AOL Instant Messenger, etc.) is prohibited except when specifically authorized by the District Superintendent (or designee).
   3. Inadvertent inappropriate access shall be reported immediately to the supervisor.

g) Expectation of Privacy
   1. Employees have no expectation of privacy in files, disks, or documents that have been created in, entered in, stored in, downloaded from, or used on district equipment.

h) Services and Assumption of Risks
   1. Erie 1 BOCES makes no warranties of any kind, whether express or implied, for services provided and is not responsible for any damages suffered while on the system to include loss of data and inaccurate or poor quality information obtained from the system. Users are responsible for backing up data stored on the hard drive of any computer assigned to them.

i) Discipline
   1. Staff members who engage in unacceptable use may lose access to the ITS (Information Technology System) and may be subject to further discipline under the law or in accordance with applicable collective bargaining agreements.
   2. Deliberate violations of this agreement (e.g., malicious acts or omissions; searching for, viewing or otherwise visiting pornographic or sexually explicit sites) are cause for disciplinary action.

j) Unacceptable Uses
   1. The following uses will be regarded as not acceptable:
      (a) Illegal or malicious use, including downloading or transmitting of copyright material.
      (b) Use for racial, sexual or other harassment in violation of district policy.
      (c) To access, view, or transmit pornographic or obscene material.
      (d) To solicit personal information with the intent of using such information to cause emotional or physical harm.
      (e) To disrupt the work of other users. This included the propagation of computer viruses and use of the Internet to make unauthorized entry to any other Internet resource.
      (f) Use for private business purposes.

k) Etiquette
   1. The following general principles should be adopted:
      (a) Be polite; do not be abusive in messages to others.
      (b) Use appropriate language: Remember that you are a representative of Erie 1 BOCES and that you are using a non-private network.
      (c) Do not disrupt the use of the Internet by other users.

(Continued)

SAMPLE FORM

Erie 1 BOCES -- Employee Computer Use Agreement (Cont'd.)

l) E-Mail massive files during peak hours and other high volume activities.
   1. Every user is responsible for all e-mail originating from their user ID (e-mail address). Forgery or attempted forgery of electronic mail is prohibited. The organization's e-mail standard (currently, Lotus Notes) is the only allowable e-mail to be used. Do not access your personal e-mail account (ex. Hotmail, AOL, etc.) through the Erie 1 network or dialup modem.
   2. Attempts to read, delete, copy or modify the e-mail of other users are prohibited.
   3. E-mail is NOT private. The District Superintendent (or designee) has the right of access to all e-mail sent or received. In the event of Erie 1 BOCES being involved in any legal proceedings, any relevant e-mails (including Internet e-mail) may have to be disclosed, on the same basis as the case for written documents.
   4. Forwarding of chain letters is not allowed.

I have read the Employee Computer Use Agreement. I understand that violation of this Agreement may be grounds for disciplinary action, including termination.

FIRST NAME _ LAST NAME _____

DIVISION _____ DEPARTMENT/PROGRAM _____

BUILDING/LOCATION _____

SIGNATURE _ DATE _____

Students

SUBJECT: STUDENT USE OF COMPUTERIZED INFORMATION RESOURCES (ACCEPTABLE USE POLICY)

The Board of Education will provide access to various computerized information resources through the District's computer system ("DCS" hereafter) consisting of software, hardware, computer networks and electronic communications systems. This may include access to electronic mail, so-called "on-line services" and the "Internet." It may include the opportunity for some students to have independent access to the DCS from their home or other remote locations. All use of the DCS, including independent use off school premises, shall be subject to this policy and accompanying regulations. Further, all such use must be in support of education and/or research and consistent with the goals and purposes of the School District.

One purpose of this policy is to provide notice to students and parents/guardians that, unlike most traditional instructional or library media materials, the DCS will allow student access to external computer networks not controlled by the School District where it is impossible for the District to screen or review all of the available materials. Some of the available materials may be deemed unsuitable by parents/guardians for student use or access. This policy is intended to establish general guidelines for acceptable student use. However, despite the existence of such District policy and accompanying guidelines and regulations, it will not be possible to completely prevent access to computerized information that is inappropriate for students. Furthermore, students may have the ability to access such information from their home or other locations off school premises. Parents/guardians of students must be willing to set and convey standards for appropriate and acceptable use to their children when using the DCS or any other electronic media or communications.

Standards of Acceptable Use

Generally, the same standards of acceptable student conduct which apply to any school activity shall apply to use of the DCS. This policy does not attempt to articulate all required and/or acceptable uses of the DCS; nor is it the intention of this policy to define all inappropriate usage. Administrative regulations will further define general guidelines of appropriate student conduct and use as well as proscribed behavior.

District students shall also adhere to the laws, policies and rules governing computers including, but not limited to, copyright laws, rights of software publishers, license agreements, and student rights of privacy created by federal and state law.

Students who engage in unacceptable use may lose access to the DCS in accordance with applicable due process procedures, and may be subject to further discipline under the District's school conduct and discipline policy and the District Code of Conduct. The District reserves the right to pursue legal action against a student who willfully, maliciously or unlawfully damages or destroys property of the District. Further, the District may bring suit in civil court against the parents/guardians of any student who willfully, maliciously or unlawfully damages or destroys District property pursuant to General Obligations Law Section 3-112.

(Continued)

SUBJECT: STUDENT USE OF COMPUTERIZED INFORMATION RESOURCES
(ACCEPTABLE USE POLICY) (Cont'd.)

Student data files and other electronic storage areas will be treated like school lockers. This means that such areas shall be considered to be School District property subject to control and inspection. The computer coordinator may access all such files and communications to ensure system integrity and that users are complying with the requirements of this policy and accompanying regulations. Students should **NOT** expect that information stored on the DCS will be private.

Notification/Authorization

The District's Acceptable Use Policy and accompanying Regulations will be disseminated to parents and student in order to provide notice of the school's requirements, expectations, and student's obligations when accessing the DCS.

*Option A: "Affirmative Consent" (Opt-in) Student use of the DCS is conditioned upon written agreement by all students and their parents/guardians that student use of the DCS will conform to the requirements of this policy and any regulations adopted to ensure acceptable use of the DCS. All such agreements shall be kept on file in the District Office.

*Option B: "Passive Consent" (Opt-out) Student access to the DCS will automatically be provided unless the parent has submitted written notification to the District that such access not be permitted. Procedures will be established to define the process by which parents may submit a written request to deny or rescind student use of the DCS in accordance with law, Commissioner's Regulations and/or District policies and procedures.

Regulations will be established as necessary to implement the terms of this policy.

NOTE: Refer also to Policy #8000 -- The Children's Internet Protection Act: Internet Content Filtering/Safety Policy

**District Option*

Adoption Date

7000F

_____ SCHOOL DISTRICT
AGREEMENT FOR STUDENT USE OF DISTRICT COMPUTERIZED INFORMATION RESOURCES

In consideration for the use of the _____ School District's Computer System (DCS), I agree that I have been provided with a copy of the District's policy on student use of computerized information resources and the regulations established in connection with that policy. I agree to adhere to the policy and the regulations and to any changes or additions later adopted by the District. I also agree to adhere to related policies published in the Student Handbook.

I understand that failure to comply with these policies and regulations may result in the loss of my access to the DCS. Prior to suspension or revocation of access to the DCS, students will be afforded applicable due process rights. Such violation of District policy and regulations may also result in the imposition of discipline under the District's school conduct and discipline policy and the Code of Conduct. I further understand that the District reserves the right to pursue legal action against me if I willfully, maliciously or unlawfully damage or destroy property of the District. Further, the District may bring suit in civil court pursuant to General Obligations Law Section 3-112 against my parents or guardians if I willfully, maliciously or unlawfully damage or destroy District property.

_____

_____

_____

_____

(Blank lines for items of student information)

_____
Student Signature

_____
Date

_____
School Building

_____ SCHOOL DISTRICT
PARENTAL/GUARDIAN CONSENT FOR STUDENT USE OF DISTRICT COMPUTERIZED INFORMATION RESOURCES

I am the parent/guardian of

_____,

the minor student who has signed the District's agreement for student use of computerized information resources. I have been provided with a copy and I have read the District's policy and regulations concerning use of the DCS.

I also acknowledge receiving notice that, unlike most traditional instructional or library media materials, the DCS will potentially allow my son/daughter student access to external computer networks not controlled by the _____ School District. I understand that some of the materials available through these external computer networks may be inappropriate and objectionable; however, I acknowledge that it is impossible for the District to screen or review all of the available materials. I accept responsibility to set and convey standards for appropriate and acceptable use to my son/daughter when using the DCS or any other electronic media or communications.

I agree to release the _____ School District, the Board of Education, its agents and employees from any and all claims of any nature arising from my son/daughter's use of the DCS in any manner whatsoever.

I agree that my son/daughter may have access to the DCS and I agree that this may include remote access from our home.

_____
Parent/Guardian Signature

_____
Date

_____ SCHOOL DISTRICT
STUDENT AND PARENT AGREEMENT

Date: _____

COMPUTER USAGE

In order to become a user of the _____ School District's computer facilities, equipment, and Internet accounts, I understand that it is necessary to comply with District policy and regulations for the use of technology as presently in force and as may be amended from time to time. A violation of the District's policy and/or regulations regarding use of computerized information resources ("Acceptable Use Guidelines") may result in the loss of computer access, disciplinary action and/or prosecution in accordance with law, regulation and/or the District Code of Conduct. I further understand that access to the computer facilities will include filtered access to the Internet.

I understand that individuals and families may be liable for violations of District policies and regulations/procedures for such use. While every reasonable effort will be made by School District personnel to monitor proper usage and provide Internet filters to questionable materials, I also accept responsibility for guidance of Internet use – setting and conveying standards for my son/daughter to follow when selecting, sharing or exploring information and media. Students who abuse the acceptable use of technology on the Internet may be removed from access in accordance with applicable due process procedures.

I have reviewed the _____ School District Acceptable Use Policy and Regulations for use of technology with my son/daughter. In consideration of the use of the _____ School District networks and in consideration for having access to the information contained on them and an Internet account, I release the _____ School District from any claims of any nature arising from my son/daughter's use of the Internet.

REQUEST TO DENY COMPUTER USAGE

In order to achieve the career development and technical education (occupational) learning standards articulated by the New York State Department of Education, students will be provided access to instructional materials and processes only available through the use of computers. I understand that if I do not request, in writing, that my child is not to use computers, an account will be created to facilitate such access. Parental requests to deny student use of District computers will be considered in accordance with law and/or regulations.

SUBJECT: THE CHILDREN'S INTERNET PROTECTION ACT: INTERNET CONTENT FILTERING/SAFETY POLICY

In compliance with The Children's Internet Protection Act (CIPA) and Regulations of the Federal Communications Commission (FCC), the District has adopted and will enforce this Internet safety policy that ensures the use of technology protection measures (i.e., filtering or blocking of access to certain material on the Internet) on all District computers with Internet access. Such technology protection measures apply to Internet access by both adults and minors with regard to visual depictions that are obscene, child pornography, or, with respect to the use of computers by minors, considered harmful to such students. Further, appropriate monitoring of online activities of minors, as determined by the building/program supervisor, will also be enforced to ensure the safety of students when accessing the Internet.

Further, the Board of Education's decision to utilize technology protection measures and other safety procedures for staff and students when accessing the Internet fosters the educational mission of the schools including the selection of appropriate teaching/instructional materials and activities to enhance the schools' programs; and to help ensure the safety of personnel and students while online.

However, no filtering technology can guarantee that staff and students will be prevented from accessing all inappropriate locations. Proper safety procedures, as deemed appropriate by the applicable administrator/program supervisor, will be provided to ensure compliance with the CIPA.

In addition to the use of technology protection measures, the monitoring of online activities and access by minors to inappropriate matter on the Internet and World Wide Web *may* include, but shall not be limited to, the following guidelines:

a) Ensuring the presence of a teacher and/or other appropriate District personnel when students are accessing the Internet including, but not limited to, the supervision of minors when using electronic mail, chat rooms, and other forms of direct electronic communications. As determined by the appropriate building administrator, the use of e-mail and chat rooms may be blocked as deemed necessary to ensure the safety of such students;

b) Monitoring logs of access in order to keep track of the web sites visited by students as a measure to restrict access to materials harmful to minors;

c) In compliance with this Internet Safety Policy as well as the District's Acceptable Use Policy, unauthorized access (including so-called "hacking") and other unlawful activities by minors are prohibited by the District; and student violations of such policies may result in disciplinary action; and

d) Appropriate supervision and notification to minors regarding the prohibition as to unauthorized disclosure, use and dissemination of personal information regarding such students.

(Continued)

SUBJECT: THE CHILDREN'S INTERNET PROTECTION ACT: INTERNET CONTENT FILTERING/SAFETY POLICY (Cont'd.)

The determination of what is "inappropriate" for minors shall be determined by the District and/or designated school official(s). It is acknowledged that the determination of such "inappropriate" material may vary depending upon the circumstances of the situation and the age of the students involved in online research.

The terms "minor," "child pornography," "harmful to minors," "obscene," "technology protection measure," "sexual act," and "sexual contact" will be as defined in accordance with CIPA and other applicable laws/regulations as may be appropriate and implemented pursuant to the District's educational mission.

**Under certain specified circumstances, the blocking or filtering technology measure(s) may be disabled for adults engaged in bona fide research or other lawful purposes. The power to disable can only be exercised by an administrator, supervisor, or other person authorized by the School District.*

The School District shall provide certification, pursuant to the requirements of CIPA, to document the District's adoption and enforcement of its Internet Safety Policy, including the operation and enforcement of technology protection measures (i.e., blocking/filtering of access to certain material on the Internet) for all School District computers with Internet access.

Notification/Authorization

The District's Acceptable Use Policy and accompanying Regulations will be disseminated to parents and students in order to provide notice of the school's requirements, expectations, and student's obligations when accessing the Internet.

*Option A: "Affirmative Consent" (Opt-in) Student use of the DCS is conditioned upon written agreement by all students and their parents/guardians that student use of the DCS will conform to the requirements of this policy and any regulations adopted to ensure acceptable use of the DCS. All such agreements shall be kept on file in the District Office.

*Option B: "Passive Consent" (Opt-out) Student access to the DCS will automatically be provided unless the parent has submitted written notification to the District that such access not be permitted. Procedures will be established to define the process by which parents may submit a written request to deny or rescind student use of District computers.

The District has provided reasonable public notice and has held at least one (1) public hearing or meeting to address the proposed Internet Content Filtering/Safety Policy prior to Board adoption. Furthermore, appropriate actions will be taken to ensure the ready availability to the public of the District's Internet Content Filtering/Safety Policy, as well as any other District policies relating to the use of technology.

47 United States Code (USC) Sections 254(h) and 254(l)
47 Code of Federal Regulations (CFR) Part 54

** and **District Option*
Adoption Date