SUBJECT: INTERNET SAFETY/INTERNET CONTENT FILTERING GUIDELINES

Internet access on the District's computer system is provided for staff and students as a means to enhance the educational mission and instructional programs of the School System, to further District goals and objectives, and to conduct research and communicate with others. In accordance with such educational mission and the instructional goals and objectives of the District, technology protection measures (i.e., filtering or blocking of access to certain material on the Internet) will be utilized on all District computers with Internet access to ensure the integrity of educational services and to address safety concerns regarding the online activities of minors. In accordance with The Children's Internet Protection Act (CIPA), the term "minor" shall mean any individual who has not attained the age of seventeen (17) years.

Consequently, the District, unless an authorized "override" (i.e., disabling of the blocking or filtering measure) is permitted as enumerated below, will block or filter Internet access for **both minors and adults** to visual depictions that are:

1) Obscene (as defined pursuant to CIPA and other applicable laws/regulations as may be appropriate);

2) Child pornography (as defined pursuant to CIPA and other applicable laws/regulations as may be appropriate);

3) For computers used by minors with Internet access, are harmful to minors. The term "harmful to minors" is defined, pursuant to CIPA, as any picture, image, graphic image file, or other visual depiction that:

   a. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

   b. Depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

   c. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

In addition, the District will monitor, as deemed appropriate by the applicable building/program administrator and/or classroom teacher, access by minors to "inappropriate matter" on the Internet and World Wide Web. Per CIPA, the District is authorized to filter or block Internet access to other material determined to be inappropriate for minors. The determination of what is "inappropriate" for

(Continued)

SUBJECT: INTERNET SAFETY/INTERNET CONTENT FILTERING GUIDELINES (Cont'd.)

minors shall be made in accordance with District guidelines and, as appropriate, on a case-by-case determination depending upon the factors such as the age of the student, the material involved, and the educational purpose/research for which such material is utilized.

However, no filtering or blocking technology has a one hundred percent (100%) guarantee that all sites accessed by staff and students are immediately filtered in compliance with law and District procedures. Consequently, if District personnel and/or students find an accessed site that is questionable, the procedure is to contact the appropriate supervisor/teacher who will notify the Superintendent/designee. The Superintendent/designee will contact, as appropriate, the service/ software provider and/or the District Technology Coordinator.

*However, 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 District is not responsible for any inappropriate content or material which may be accessed via a staff member's or a student's own personal technology or electronic device or via an unfiltered Internet connection received through a staff member's or a student's own personal technology or electronic device.

Further, in order to help ensure the safety and security of minors when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications, appropriate supervision will be provided by a classroom teacher and/or other appropriate District personnel; and notification will be given to minors regarding the prohibition as to unauthorized disclosure, use and dissemination of personal identification information regarding such students. Students will also be informed regarding unauthorized access to District computers and the Internet, including so-called "hacking," and other unlawful activities by minors online.

Parental and/or student consent, as may be applicable, shall be required prior to authorization for student use of District computers as a means to help ensure awareness/compliance with District rules and standards of acceptable behavior.

In accordance with New York State Education Law, the School District may provide, to students in grades kindergarten through twelve (12), instruction designed to promote the proper and safe use of the Internet. Schools must instruct students in appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, as well as providing education on

**District Option*

(Continued)

SUBJECT: INTERNET SAFETY/INTERNET CONTENT FILTERING GUIDELINES (Cont'd.)

cyberbullying awareness and response. The Commissioner shall provide technical assistance to assist in the development of curricula for such course of study which shall be age appropriate and developed according to the needs and abilities of students at successive grade levels in order to provide awareness, skills, information and support to aid in the safe usage of the Internet.

In furtherance of the District's educational mission to enact safety measures to protect students when online, the District has adopted and will enforce its Internet Safety Policy that includes the operation of technology protection measure(s) with respect to any of its computers with Internet access as mandated by CIPA and also in accordance with the District's Acceptable Use Policies and Regulations. The District shall enforce the operation of such technology protection measure(s) during any use of District computers in accordance with CIPA and applicable Board policies and building procedures.

Furthermore, in accordance with law, the District Technology Coordinator may access all staff and student files, email, and electronic storage areas to ensure system integrity and that users are complying with the requirements of CIPA and District policy and procedures. Additionally, dissemination and/or publication of the District's Acceptable Use Policy and Regulation will be utilized as one means to further ensure the implementation of safety measures and appropriate notification to staff and students as to acceptable, as well as prohibited, conduct when using District computers or accessing the Internet on such computers. The standards of acceptable use as well as prohibited conduct by staff and students when accessing District computers and the Internet, as outlined in the District's technology policies, are not intended to be all-inclusive. Staff and students who commit an act of misconduct which is not specifically addressed in District policy and/or regulation may also be subject to disciplinary action in accordance with law, the District Code of Conduct, and/or the applicable collective bargaining agreement. Legal action may also be initiated as deemed necessary by the Superintendent/designee.

DEPEW UNION FREE SCHOOL DISTRICT
INTERNET CONTENT FILTERING - AUTHORIZED "OVERRIDE" OPTION FORM

In accordance with The Children's Internet Protection Act, authorization may be granted by the designated school official(s) to disable blocking or filtering measures on District computers to enable access by **adults** engaged in bonafide research or other lawful purposes. The power to disable can only be exercised by an administrator, supervisor, or other person authorized by the District. There may be special projects/research done on the Internet where, for a limited period of time, filtering needs to be "turned off" to allow access to particular web sites. The capability of setting the time period to be "unfiltered," as well as the changing of the password, will reside with the person authorized to possess this user ID.

Only the designated authorized person will have the use of the user ID and password and will not share this information with the staff. Please provide the information below to the authorized designated person for approved "override" (i.e., disabling of technology protection measures). This form must be completed and submitted at least five (5) school days in advance.

AUTHORIZED OVERRIDE CAPABILITY WILL BE PROVIDED IN ACCORDANCE WITH THE PROVISIONS OF THE SCHOOL DISTRICT'S INTERNET CONTENT FILTERING/ SAFETY POLICY.

Please fill out the form below to request the authorized override option.

Staff Member's Name:_____

Date of Application:_____

Date(s)/Times/Location of Override:_____

_____

Purpose for Override Request (be specific): _____

_____

Staff Person's Signature:_____

Staff Person's Internet Address:_____

Title of Authorized Staff Member _____

Signature of Authorized Staff Member:_____