USE OF COMPUTERIZED INFORMATION RESOURCES & ACCEPTABLE USE POLICY

The Board of Education believes that providing access to technology is an integral part of a contemporary education. Within financial limitations, computers, computer networks and the internet will be made available to students, faculty and staff. The technology resources at the School District (e.g., all networking, hardware and software, the Internet, e-mail, telephone equipment, digital still and video, voice mail, fax machines and supporting telephone lines, and all communication equipment) are provided to support the educational and administrative activities of the School District and should be used for those purposes. An individual's use of the School District's computer resources must be in support of education and research and consistent with the educational objectives of the School District.

When an individual accesses computers, computer systems and/or computer networks, including the internet (hereinafter the "School District's computer resources") provided by the School District, he/she assumes certain responsibilities and obligations. Access to the School District's computers, computer systems and/or computer networks is subject to federal, state and local law, as well as Board of Education policy. The use of the School District's computers, computer networks and the internet is a privilege, not a right, and inappropriate use will result in the cancellation of privileges and/or disciplinary action by School District officials.

Authorized Use

Authorized users of the School District's computer resources include members of the Board of Education, administrators, supervisors, faculty, staff, students and any other person who has been granted authority by the School District to access its computing, network and telephone systems and whose usage complies with this policy. All School District business being conducted via email must be performed with a School District account. All School District business being conducted via email must be performed with a School District account. Unauthorized use is strictly prohibited.

Faculty, staff members and students may be provided with e-mail accounts and Internet access. Staff members may also be provided with e-mail accounts, voice mail accounts, Internet access and other telecommunications upon approval of their supervisors. Whenever a user ceases being a member of the School District community or if such user is assigned a new position and/or responsibilities, use of the School District's computer resources for which he or she is not authorized in his or her new position or circumstances shall cease and property returned. When a School District employee separates from service from the School District, access to all School District accounts and email is disabled.

Privacy Expectations

The School District's computer resources, including all telephone and data lines, are the property of the School District. The School District reserves the right to access, view or monitor any information or communication stored on or transmitted over the network, or on or over equipment that has been used to access the School District's computer resources. **There is no guarantee of privacy associated with an individual's use of the School District's computer**

resources. Users should not expect that e-mail, voice mail or other information created or maintained in the system (even those marked "personal" or "confidential") are private, confidential or secure.

Responsible Use

1. All users must act in ways that do not invade the privacy of others and comply with all legal restrictions regarding the use of electronic data.

2. All users must maintain the confidentiality of student information in compliance with federal and state law. Disclosing and/or discussing (including but not limited to via e-mail, voice mail, Internet instant messaging, chat rooms or on Web pages) about confidential or proprietary information related to the School District is prohibited.

3. All users must refrain from acts that waste the School District's computer resources or prevent others from using them. Users will not access, modify or delete others' files or system settings without express permission. Tampering of any kind is strictly forbidden. Deliberate attempts to tamper with, circumvent filtering or access, or degrade the performance of the School District's computer resources or telephone system or to deprive authorized users of access to or use of such resources are prohibited.

4. Users are responsible for both the content and possible effects of their messages on the School District's computer resources. Prohibited activity includes, but is not limited to, creating or propagating viruses, material in any form (text, sound, pictures or video) that reflects adversely on the School District, "chain letters" (which proffer incentives to relay them to others), inappropriate messages (including discriminatory, bullying, cyberbullying or harassing material), and billable services.

5. Official email communications must be professional, ethical and meet the standards of other School District publications bearing in mind that the writer is acting as a representative of the School District and in furtherance of the School District's educational mission.

6. Users are prohibited from using personal links and addresses such as blogs, YouTube videos, etc. in School District email unless used in the furtherance of the business of the School District or as part of the curriculum of the School District. The signature portion of the user's email may not include external links or graphics that are unrelated to the content of the email.

7. Altering electronic communications to hide the identity of the sender or impersonate another person is illegal, considered forgery and is prohibited.

8. Users will abide by all copyright, trademarks, patent and other laws governing intellectual property. No software may be installed, copied or used with or on the School District's computer resources except as permitted by law and approved by the District Director of Technology or his/her designee. All software license provisions must be strictly adhered to.

9. Since the installation of applications, other than School District-owned and School District-tested programs could damage the School District's computer resources or interfere with others' use, software downloaded from the Internet or obtained elsewhere must be approved by the District Director of Technology or his/her designee. Software may not be installed onto any School District owned or School District-leased computer by an individual other than the District Director of Technology or his/her designee.

10. Use of voice mailboxes for commercial purposes or advertising is not permitted. Use of security codes is required in order to guarantee privacy for mailbox users.

Inappropriate Materials

1. The School District prohibits faculty, staff, students and individuals visiting the School District from developing, maintaining, and transmitting pornography in any form at school, including, but not limited to, magazines, posters, videos, electronic files or other electronic materials.

2. Accessing the School District's computer resources to create, access, download, edit, view, store, send or print materials that are illegal, offensive, harassing, intimidating, discriminatory, sexually explicit or graphic, pornographic, obscene, or which constitute sexting or cyberbullying or are otherwise inconsistent with the values and general standards for community behavior of the School District is prohibited. The School District will respond to complaints of harassing or discriminatory use of its computer resources in accordance with its Anti-Harassment and Anti-Discrimination Policies.

General Criteria for Web Page Publishing

The availability of Internet access in the School District provides an opportunity for staff and students to access information and contribute to the School District's presence on the World Wide Web. The District/school/classroom websites must relate to curriculum or instructional matters, school authorized activities, or general information of interest to the public pertaining to the District or its schools. Staff and students are prohibited from publishing personal home pages or links to personal home pages as part of the District/school/classroom Web Page(s). Similarly, no individual or outside organization will be permitted to publish personal Web Pages as part of the District/school/classroom Web Page(s).

Internet access for the creation of Web Pages is provided by the District and all information must be reviewed by the Director of Technology or his/her designee prior to publishing it on the Web. Personnel designing information for the Web Pages must familiarize themselves with and adhere to District standards and procedures, as set forth in the accompanying Regulations. Failure to follow District standards or responsibilities may result in disciplinary sanctions in accordance with law and/or the applicable collective bargaining agreement.

The District may provide, as necessary, general training on relevant legal considerations and compliance with applicable laws and regulations including copyright, intellectual property, and privacy of student records as well as relevant District procedures to those staff members and

students who are allowed to develop or place material on the District/school/classroom Web Page(s).

Social Media Guidelines for Professional Use

The School District recognizes the importance of an open exchange between the district and its many constituents. Likewise, the District recognizes social media as an important arena for encouraging interaction and collaboration. The School District has established Regulations to address procedures and best practices for professional-use social media accounts created to represent District groups, departments, programs, etc., and the District as a whole, and do not apply to personal/individual accounts. The district reserves the right to block any users and/or comments for any abusive, offensive or inappropriate language.

"Social Media": Includes all methods of interaction online in all forms of user generated and distributed content, including but not limited to, blogs, social networking sites and applications (including Facebook, Twitter, Snapchat, Instagram, YouTube, gaming and any other applications).

"Professional Use": Refers to the creation of an approved social media account to advance a program or function of the School District. Content includes or reflects the opinions or representation of the District or group within/governed by the District.

Use of Personal Electronic Devices

The Board of Education authorizes use of personal electronic device(s) to access the internet using the School District's computer resources for educational purposes. Individuals connecting to the internet using the School District's computer resources are required to comply with the School District's Internet Safety Policy, as well as the provisions of this policy and regulation. Failure to abide by this policy and regulation will result in disciplinary action including, but not limited to, revocation of access to the School District's computer resources.

"Personal electronic devices" include, but are not limited to, personal laptops, smart phones, portable storage media, all recording devices, all Internet connected devices and handheld devices such as iPods and iPads. With classroom teacher approval, students may use their own devices to access the Internet for educational purposes. The School District reserves the right to monitor, inspect, and/or confiscate personal electronic devices when administration has reasonable suspicion that a violation of school policy has occurred.

The School District maintains a "public" wireless network, a "private" wireless network and a "hard wired" network. The "hard wired" and "private" wireless networks are limited only to district-owned and managed devices. Any attempt to connect a personal electronic device to either of these networks will be considered a violation of this policy. The "public" wireless network is the sole network that students and faculty may connect to using their personal electronic devices. The School District reserves the right to alter or disable access to the "public" wireless network as it deems necessary without prior notification.

Personal electronic devices that have the ability to offer wireless access to other devices must not

be used to provide that functionality to others in any School District building. The ability to connect personal electronic devices to the School District wireless network is a privilege and not a right. When personal electronic devices are used in School District facilities or on the School District wireless network, the School District reserves the right to:

1. make determinations on whether specific uses of the personal electronic device is consistent with this policy;

2. log internet use and monitor storage disk space utilized by such users; and

3. remove or restrict the user's access to the internet and suspend the right to use the personal electronic device in School District facilities at any time if it is determined that the user is engaged in unauthorized activity or in violation of Board of Education policy.

In addition, when staff members choose to use their own personal electronic devices to perform job-related functions, the following will apply:

1. The School District may choose to maintain a list of approved mobile devices and related software applications and utilities. The School District reserves the right to deny any staff member permission to utilize a personal electronic device within the boundaries of the School District. The Superintendent of Schools or his/her designee reserves the right to make these decisions as necessary.

2. Personal electronic devices connected to the internet using the School District's computer resources and/or wireless network must have updated and secure operating systems and proper forms of anti-virus and anti-malware protection. Staff must not make any attempt to connect devices that are not properly secured.

3. The cost to acquire all personal electronic devices is the responsibility of the staff member. Services that include a financial cost to the School District, such as phone options or other "apps" are not allowed. The School District does not agree to pay such charges and staff who desire these options must assume all costs incurred for such charges.

4. Personal electronic devices are not covered by the School District's insurance if lost, stolen or damaged. Loss or damage to any personal electronic device is solely the responsibility of the staff member. If lost or stolen, the loss should be reported immediately to District's Director of Technology so that appropriate action can be taken to minimize any possible risk to the School District's computer system and the School District.

5. Staff members shall remain responsible for the maintenance of personal electronic devices, including maintenance to conform to School District standards. Staff members also assume all responsibility for problem resolution, as well as the use and maintenance of functional, up-to-date anti-virus and anti-malware software and any other protections deemed necessary by the District Director of Technology or his/her designee.

6. Staff must also meet any expectations of continuity in formatting of files, etc. when making changes to documents for work purposes (i.e., do not change the format of a file

so that the original file is unusable on School District-owned hardware/software).

7. All personal electronic devices used with the School District's computer resources is subject to review by the District Director of Technology, or individuals/entities designated by the Superintendent of Schools, if there is reason to suspect that the personal electronic device is causing a problem to the School District's computer resources.

8. The use of personal electronic devices in the course of a staff member's professional responsibilities may result in the equipment and/or certain data maintained on it being subject to review, production and/or disclosure (i.e., in response to a FOIL request, discovery demand or subpoena). Staff members are required to submit any such information or equipment, when requested.

9. Staff members using a mobile device, personal or District-owned, are responsible for ensuring that all security protocols normally used in the management of School District data on conventional storage infrastructure are also applied on that mobile device. All School District-defined processes for storing, accessing and backing up data must be used on any device used to access the School District's computer system.

Further, the School District will not be liable for the loss, damage, theft, or misuse of any personal electronic device(s) brought to school. The School District will bear no responsibility nor provide technical support, troubleshooting, or repair of electronic devices owned by anyone other than the School District. Students and staff are responsible for understanding and inquiring about the use of technology prior to engaging in such use.

Confidentiality and Privacy Rights

Individuals must take all reasonable precautions to prevent unauthorized access to accounts or data by others, both inside and outside the School District. Individuals will not leave any devices unattended with confidential information visible. All devices are required to be locked down when an individual steps away from the device, and settings enabled to freeze and lock after a set period of inactivity.

Data files and electronic storage areas shall remain School District property, subject to School District control and inspection. The District Director of Technology may access all such files and communications without prior notice to ensure system integrity and that users are complying with requirements of this policy.

Security

1. Each user is responsible for the security and integrity of information stored on his or her computer or voice mail system. Computer accounts, passwords, security codes and other types of authorization are assigned to individual users and must not be shared with or used by others. The School District, at its sole discretion, reserves the right to bypass such passwords and to access, view or monitor its systems and all of their contents. By utilizing the School District's computer resources, the user has

consented to the School District's right to access any and all information thereon.

2. Removing or relocating School District-owned computer resources require prior authorization from the District Director of Technology or his/her designee.

3. Users may not attempt to circumvent or subvert the security provisions of any other system. No one may attach a server to or provide server services on the School District network.

School District Limitation of Liability

The School District does not warrant in any manner, express or implied, that the functions or the services provided by or through the School District system will be error-free or without defect. The School District shall not bear any liability for any damage suffered by users including, but not limited to, loss of data or interruption of service. Similarly, the School District shall not bear any liability for financial obligations that arise out of the unauthorized or illegal use of the system.

Users of the School District's computer resources, including internet use, do so at their own risk. Each user is responsible for verifying the integrity and authenticity of the information that is used and provided. Further, even though the School District may use technical or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of the Board of Education and School District policy and regulations.

Sanctions

1. There are risks involved with using the Internet. To protect personal safety, Internet users should not give out personal information to others on website, chat rooms or other systems. The School District cannot guarantee that users will not encounter text, pictures or references that are objectionable. Responsible attitudes and appropriate behavior are essential in using this resource. As with e-mail, information that a user places on the Internet is akin to sending a postcard rather than a sealed letter. Its contents may be accessed by system administrators in the School District and elsewhere.

2. Users must be aware that some material circulating on the Internet is illegally distributed. Users must never use the School District's computer resources to download illegally distributed material.

3. Users are cautioned not to open e-mail attachments or download any files from unknown sources in order to avoid damage to the School District's computer resources. Anything questionable should be reported immediately to the District Director of Technology or his/her designee.

4. With permission, students, faculty and staff may create or modify web pages on the School District web servers which comply in all respects with this policy.

All members of the School District community are expected to assist in the enforcement of this

policy. Persons in violation of this policy are subject to a full range of sanctions, including, but not limited to, the loss of computer, telephone or network access privileges, disciplinary action, and dismissal/termination from the School District. Some violations may constitute criminal offenses as defined by local, state and federal laws, and the School District may initiate or assist in the prosecution of any such violations to the full extent of the law.

Any suspected violation of this policy should be reported immediately to the District Director or Technology or his/her designee and the Superintendent of Schools. Anyone receiving a threatening message should record/save the message and report the incident to the Principal. The District Director of Technology or his/her designee will attempt to trace the message and report the results to the Principal and the Superintendent of Schools.

Cross Ref:

Ref:

Adoption Date:

The following guidelines list examples of behaviors which the Board of Education considers inappropriate uses of the School District's computer resources, including the internet. Students, staff and faculty using the School District's computer resources or personal electronic devices to access the Internet will refrain from the prohibited activities. Prohibited activities include, but are not limited to:

- the use of impolite, abusive, inappropriate, or otherwise objectionable language, pictures or images in in either public or private e-mail messages, text messages, or website postings.
- placing unlawful information on the internet
- using the Internet illegally in ways that violate federal, state, or local laws or statutes;
- using the Internet at school for non-school related activities;
- sending messages that are likely to result in the loss of the recipient's work or systems;
- sending chain letters or pyramid schemes to lists or individuals or any other types of use which would cause congestion of the Internet or otherwise interfere with the work of others;
- using the Internet for commercial purposes;
- using District email to sell personal property;
- using the internet for shopping purposes;
- using District email to advertise your personal business;
- using the Internet to lobby for political candidates;
- changing any computer file that does not belong to the user;
- sending or receiving copyrighted materials without permission;
- plagiarizing information found on the Internet:
- knowingly giving one's password to others;
- using another person's password;
- using Internet access for sending or retrieving pornographic material, inappropriate text files, or files dangerous to the integrity of the network;
- circumventing security measures or school or remote computers or networks;
- attempting to gain access to another's resources, programs, or data;
- vandalizing, which is defined as any malicious attempt to harm or destroy data of another user on the Internet, and includes the uploading or creation of computer viruses;
- falsifying one's identity to others while using the Internet;
- giving one's personal home address or phone number or the personal home address or phone number of any other student while using the Internet;
- using the Internet for purposes of cyber-bullying, such as harassing, teasing, intimidating or threatening another student or staff member.

Further, the School District's computer resources may be used only for authorized purposes following established procedures. Inappropriate use of School District computer resources is prohibited. The following constitutes a non-exhaustive list of actions that are considered inappropriate:

- using another person's password;
- using another person's files, system, or data without permission;
- using computer programs to decode passwords or to access control information;
- attempting to circumvent or subvert system security measures;
- accessing any programs specifically designed for use by the system administrator;
- engaging in any activity that might be harmful to systems or to any information stored thereon, such as creating viruses, damaging files, or disrupting service;
- making or using illegal copies of copyrighted software, storing such copies on school systems, or sending them over networks;
- using mail service to harass others;
- wasting computing resources;
- engaging in any activity that does not comply with the general principles listed at the beginning of this document;
- violating any condition of the Board of Education's policies.

Monitoring of School District Sponsored Social Media Accounts

The District Director of Technology is responsible for reviewing and approving all Professional Use social media site/account applications for the District, in consultation with the Superintendent of Schools, and members of the district leadership team.

The Director of Technology reserves the right to remove or direct the removal of content posted to, or within the comment sections of, a Professional Use social media site/account that:

- Is off-topic;
- Contains personal attacks;
- Contains spam;
- Contains discriminatory, defamatory or harassing language;
- Contains confidential information;
- Violates the property rights of others (such as when an account is hacked or used by another person, or violates copyright laws).

Appropriate Use When Utilizing Social Media

District employees are expected to follow the same behavioral standards online as they would at work. The same professional expectations and guidelines for interacting with students, parents, alumni, district staff, media and other District stakeholders apply online as in the real world. Employees should note the following guidelines:

- Follow the professional Code of Ethics.
- Discourage and remove content posted to, or within the comment sections of, the Professional Use social media site/account that:
- Is off-topic;
- Contains personal attacks;
- Contains spam;
- Contains discriminatory, defamatory or harassing language;
- Contains confidential information;

- Violates the property rights of others (such as when an account is hacked or used by another person, or violates copyright laws).
- Staff members are encouraged to share items posted to the District website or Facebook page. Employees with information and news to announce to the public or media should contact the District communications specialist.
- Remember that District computers and resources are to be used only for job-related purposes and educational purposes for students, as set forth in this policy.
- Respect copyright and fair use: when posting, be mindful of the copyright and intellectual property rights of others and of the School District.
- Guidelines regarding use of student photographs and information apply to online publications, including social media.
- Students' and employees' addresses, telephone numbers and other confidential information should never be posted online or on social media websites.

Content Standards for Web Page Publishing

1. Approval for posting a Web Page must be obtained from the Director of Technology or his/her designee. If at any time, the Director or his/her designee believes the proposed material does not meet the standards approved by the District, it will not be published on the Web. Decisions regarding access to active Web Pages for editing content or organization will be the responsibility of the Director of Information Services/designee(s).
2. A Web Page must be sponsored by a member of the District faculty, staff or administration who will be responsible for its content, design, currency and maintenance. The sponsor is responsible for ensuring that those constructing and maintaining the Web Page have the necessary technical training and that they fully understand and adhere to District policies and regulations. The Web Page must include the name of the sponsor.
3. Staff or student work should be published only as it relates to a school/classroom authorized project or other school-related activity.
4. The review of a Student Web Page shall be subject to prior District review as would any other school-sponsored student publication.
5. An authorized teacher, staff member or administrator who is publishing the final Web Page(s) for himself/herself or for a student will edit and test the Page(s) for accuracy of links and check for conformance with District standards and practices.
6. The following disclaimer about the content of Web Pages must be part of individual sites: "The District has made every reasonable attempt to ensure that our Web Pages are educationally sound and do not contain links to questionable material or material that can be deemed in violation of the District's Standards and Guidelines for Web Page Publishing Policy and the Acceptable Use Agreement."
7. Commercial advertising or marketing on the District/school/classroom Web Page(s) (or the use of school-affiliated Web Pages for the pursuit of personal or financial gain) shall be prohibited unless otherwise authorized in accordance with law and/or regulation. Decisions regarding website advertising must be consistent with existing District policies and practices on this matter. School-affiliated Web pages may mention outside organizations only in the context of school programs that have a direct relationship to those organizations.
8. Web Pages may include faculty or staff names; however, other personal information about employees including, but not limited to, home telephone numbers, addresses, email

addresses, or other identifying information such as names of family members may be published only with the written permission of the employee.

9. All Web Pages must conform to the standards for appropriate use found in the District's Acceptable Use Policy and accompanying Regulations regarding standards of acceptable use; examples of inappropriate behavior; and compliance with applicable laws, privacy, and safety concerns.
10. All Web Pages must be approved through the designated process before being posted to the District/school/classroom websites.
11. All staff and/or students authorized to publish material on the District/school/classroom Web Page(s) shall acknowledge receipt of the District's Web Page Standards and agree to comply with same prior to posting any material on the Web.

Use of Copyrighted Materials and "Fair Use" Exceptions/Intellectual Property and Works Made for Hire

Copyrighted Materials

All employees and students are prohibited from copying materials not specifically allowed by the copyright law, "Fair Use" guidelines, licenses or contractual agreements, or the permission of the copyright proprietor. Web Page publications must include a statement of copyright when appropriate and indicate that permission has been secured when including copyrighted materials or notice that such publication is in accordance with the "Fair Use" provisions of the Copyright Law.

Fair Use of Copyrighted Materials

Pursuant to Section 107 of the Copyright Law ("Fair Use" provisions), the use of copyrighted material for criticism, comment, news reporting, teaching, scholarship, or research may be permitted under certain circumstances.

However, any appropriation of someone else's work on the Internet is a potential copyright infringement. "Fair Use" provisions may not apply when a project created by a teacher or student is accessed by others over the Internet. If there is a possibility that school-affiliated Web Page(s), which incorporate copyrighted works under the "Fair Use" provisions, could later result in broader dissemination, it will be necessary to seek the permission of the copyright holder. The complex interplay between copyright law and the "Fair Use" provisions in educational multimedia projects should be considered in development of Web Page publishing standards and reviewed by school counsel prior to District implementation for compliance with applicable law and regulations.

1. Unless otherwise noted, always assume that work on the web is copyrighted. It is NOT necessary that the copyright symbol -- © -- be displayed for the work to be protected by copyright laws.
2. Proper attribution must always be given.
3. Obtaining permission(s) from the copyright holder(s) (whether text, graphics or music) should occur during the developmental process or project, rather than waiting to seek permission upon completion of the project.

Intellectual Property/Works Made for Hire

All works completed by employees as part of their employment shall be considered "works made for hire" as described in the United States Code Annotated, Title 17, Copyrights to the extent permitted by law. This determination includes, but is not limited to, the following activities:

1. Work prepared by an employee within the scope of his/her employment, whether tangible or intangible;
2. Work specifically ordered or commissioned for use as a contribution to a collective work, as enumerated in law.

Any work created within the scope of such a relationship will be considered a work made for hire when a regular employment relationship exists.

Work covered under this policy is the property of the School District, not the creator of such work. The District shall own any and all rights to such works, or derivatives thereof, unless there is a written agreement to the contrary.

Students

*Students are the copyright holders of their own original work. The District must receive written permission from both the parent and the student prior to publishing students' original work on the District/school/classroom websites.

Students posting non-approved or inappropriate material on a school-affiliated website are subject to the imposition of discipline, including possible suspension or revocation of access to the District's computer network, in accordance with applicable due process procedures and the District Code of Conduct. In the case that a violation may constitute a criminal offense, it will be reported to the appropriate authorities.

*Students must be sponsored and supervised by a member of the teaching staff. Students will not have access to login information for Web Pages.

Staff

Faculty or staff posting non-approved or inappropriate material on a school-affiliated website are subject to the imposition of discipline, including, but not limited to, possible suspension or revocation of access to the District's network. The Superintendent of Schools or his/her designee shall have the authority to approve or deny the posting of any proposed Web Pages on school-affiliated websites based upon compliance with the terms and conditions set forth in this policy as well as applicable District practices and procedures.

Consequences for Non-Compliance

Web pages that do not comply with the above criteria are subject to revocation of approval and removal from the District/school/classroom websites.

Education Law Section 2-D Definitions

"Educational agency" means a school district, board of cooperative educational services, school, or the education department.

"Personally identifiable information, (PII)," as applied to student data, means personally identifiable information as defined in section 99.3 of title thirty-four of the code of federal regulations implementing the family educational rights and privacy act, section twelve hundred thirty-two-g of title twenty of the United States code, and, as applied to teacher or principal data, means "personally identifying information" as such term is used in subdivision ten of section three thousand twelve-c of this chapter.

"School" means any public elementary or secondary school, universal pre-kindergarten program authorized pursuant to section thirty-six hundred two-e of this chapter, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in section four thousand one of this chapter, an approved private school for the education of students with disabilities, a state-supported school subject to the provisions of article eighty-five of this chapter, or a state-operated school subject to the provisions of article eighty-seven or eight-eight 1 of this chapter.

"Student" means any person attending or seeking to enroll in an educational agency.

"Eligible student" means a student eighteen years or older.

"Parent" means a parent, legal guardian, or person in parental relation to a student.

"Student data" means personally identifiable information from student records of an educational agency.

"Teacher or principal data" means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of section three thousand twelve-c of this chapter.

"Third party contractor" shall mean any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities pursuant to section two hundred eleven-e of this title and is not an educational agency as defined in paragraph c of this subdivision, and a not-for-profit corporation or other non-profit organization, other than an educational agency.

What Data is Protected?

The law limits collection and use of student data, defined as personally identifiable information from student records of an educational agency. Personally identifiable information is defined in the same manner as in FERPA. The law also limits collection and use of personally identifiable information relating to the annual professional performance reviews of classroom principals or teachers.

These policies will include:

1. Data privacy protections, including criteria for determining whether a proposed use of PII would benefit students and educational agencies, and processes to ensure that PII is not included in public reports or other public documents;
2. Data security protections, including data systems monitoring, data encryption, incident response plans, limitations on access to personally identifiable information, safeguards to ensure personally identifiable information is not accessed by unauthorized persons when transmitted over communication networks, and destruction of personally identifiable information when no longer needed; and
3. Application of all such restrictions, requirements and safeguards to third-party contractors.