Exhibit A
12,13,15
10 pgs
(not including memo)

Lockport City School District

130 Beattie Avenue, Lockport, New York 14094-5099
Lisa M. Schrader
Assistant Superintendent for Personnel

Fax:
Phone: [redacted]
http://www.lockportschools.org

TO: Debbie
FROM: Lisa Schrader
DATE: June 20, 2018
RE: FOIL request documents

Attached are the documents to assist with responding to the FOIL request from NYCLU. The policies and Parents Bill of Rights Document may serve to address items 12, 13, and 15 on the FOIL request.

"Pride in Our Past; Faith in Our Future"

The Lockport City School District (LCSD) does not discriminate against any employee, student, applicant for employment, or candidate for enrollment on the basis of gender, race, color, religion or creed, age, national origin, marital status, disability or any other classification protected by law. LCSD is a drug-free workplace. This policy includes: access by students to educational and vocational programs, counseling services for students, course offerings, and student activities; as well as recruitment and appointment of employees and employment pay, benefits, advancement and/or termination.

LCSD 000143

SUBJECT: USE OF SURVEILLANCE CAMERAS IN THE SCHOOL DISTRICT AND ON SCHOOL BUSES

It is the Board of Education's responsibility to ensure the safety of the District's students, staff, facilities, and property. While the Board of Education recognizes the importance of privacy, it has authorized the use of surveillance cameras on District property including in school buildings, school facilities, as well as on school buses, when necessary. These surveillance cameras will help to assist the Board in maintaining the overall safety and welfare of the District's students, staff, property, and visitors, as well as to deter theft, violence, and other criminal activities.

Further, surveillance cameras will only be placed in public or common areas, such as stairwells, hallways, cafeterias, parking lots, or playgrounds, and not in private areas such as locker rooms, bathrooms, or other areas in which individuals have a reasonable expectation of privacy. The District officials will not utilize audio recordings, however, this prohibition may not preclude the use of audio recordings by law enforcement officials in accordance with their official duties or as otherwise authorized by law.

Disciplinary Proceedings

Video recordings or footage from District surveillance cameras may be used in student or employee disciplinary proceedings, as appropriate.

Signage/Notification

The District will place signage at entrances to the school campus or at major entrances into school buildings notifying students, staff, as well as any visitors of the District's use of surveillance cameras. Students and staff will also receive additional notification, as deemed appropriate by the Superintendent, regarding the use of its surveillance cameras through means such as publication in the District calendar, employee handbook, and/or the student handbook.

Maintenance of Video Recordings

Any video surveillance recording in the schools, on school buses, or on school property, on tape, CD, or digitally, will be the sole property of the District and stored in its original form and in a secure location to avoid tampering and also to ensure its confidentiality in accordance with relevant law and regulations.

In addition, to the extent that any video images create student or personnel records, the District will comply with all applicable state and federal laws related to record retention, record maintenance, and record disclosure, including the Family Educational Rights and Privacy Act ("FERPA").

BOE Adoption Date – October 2016

SUBJECT: DATA NETWORKS AND SECURITY ACCESS

The District values the protection of private information of individuals in accordance with applicable law, regulations, and best practice. Accordingly, District officials and Information Technology (IT) staff will plan, implement, and monitor IT security mechanisms, procedures, and technologies necessary to prevent improper or illegal disclosure, modification, or denial of sensitive information in the District Computer System (DCS). Similarly, such IT mechanisms and procedures will also be implemented in order to safeguard District technology resources, including computer hardware and software. District network administrators may review District computers to maintain system integrity and to ensure that individuals are using the system responsibly. Users should not expect that anything stored on school computers or networks will be private.

In order to achieve the objectives of this policy, the Board of Education entrusts the Superintendent, or his/her designee, to:

a) Inventory and classify personal, private, and sensitive Information on the DCS to protect the confidentiality, integrity, and availability of information;

b) Develop password standards for all users including, but not limited to, how to create passwords and how often such passwords should be changed by users to ensure security of the DCS;

c) Ensure that the "audit trail" function is enabled within the District's network operating system, which will allow the District to determine on a constant basis who is accessing the DCS, and establish procedures for periodically reviewing such audit trails;

d) Develop procedures to control physical access to computer facilities, data rooms, systems, networks, and data to only authorized individuals; such procedures may include ensuring that server rooms remain locked at all times and the recording of arrival and departure dates and times of employees and visitors to and from the server room;

e) Establish procedures for tagging new purchases as they occur, relocating assets, updating the inventory list, performing periodic physical inventories, and investigating any differences in an effort to prevent unauthorized and/or malicious access to these assets;

f) Periodically grant, change, and terminate user access rights to the overall networked computer system and to specific software applications and ensure that users are given access based on, and necessary for, their job duties;

g) Limit user access to the vendor master file, which contains a list of vendors from which District employees are permitted to purchase goods and services, to only the individual who is responsible for making changes to such list, and ensure that all former employees' access rights to the vendor master list are promptly removed;

(Continued)

SUBJECT: DATA NETWORKS AND SECURITY ACCESS (Cont'd.)

h) Determine how, and to whom, remote access should be granted, obtain written agreements with remote access users to establish the District's needs and expectations, as appropriate, and monitor and control such remote access;

i) Verify that laptop computer systems assigned to teachers and administrators use full-disk encryption software to protect against loss of sensitive data;

j) Deploy software to servers and workstations to identify and eradicate malicious software attacks such as viruses and malware;

k) Develop a disaster recovery plan appropriate for the size and complexity of District IT operations to ensure continuous critical IT services in the event of any sudden, catastrophic event, including, but not limited to fire, computer virus or deliberate or inadvertent employee action.

**Customize to District -- intended as a template that should be customized to District practices as applicable.*

Adoption Date: November 4, 2015

/EB

SUBJECT: STUDENT DATA BREACHES

A student data breach is defined as any instance in which there is an unauthorized release of or access to personally identifiable information (PII) or other protected information of students not suitable for public release.

School districts have a legal responsibility to protect the privacy of education data, including personally identifiable information (PII) of its students. The Family Education Rights and Privacy Act of 1974, commonly known as FERPA, protects the privacy of student education records. Although FERPA does not include specific data breach notification requirements, it does protect the confidentiality of education records and requires districts to record each incident of data disclosure in accordance with 34 CFR 99.32 (a)(1). In addition, under state law, direct notification of parents and/or affected students may be warranted depending on the type of data compromised, such as student social security numbers and/or other identifying information that could lead to identity theft.

The District has implemented privacy and security measures designed to protect student data stored in its student data management systems. These measures include reviewing information systems and data to identify where personally identifiable information is stored and used; monitoring data systems to detect potential breaches; and conducting privacy and security awareness training for appropriate staff. In the event of an alleged breach, the District will promptly take steps to validate the breach, mitigate any loss or damage, and notify law enforcement if necessary.

The Superintendent will develop and implement regulations for prevention, response and notification regarding student data breaches.

34 CFR 99.32 (a)(1)
Technology Law Sections 202 and 208

NOTE: Refer also to Policies #5672 -- Information Security Breach and Notification
#7240 -- Student Records: Access and Challenge

Adoption Date: November 4, 2015

SUBJECT: CONFIDENTIALITY OF COMPUTERIZED INFORMATION

The development of centralized computer banks of educational data gives rise to the question of the maintenance of confidentiality of such data while still conforming to the New York State Freedom of Information Law. The safeguarding of confidential data from inappropriate use is essential to the success of the District's operation. Access to confidential computerized data shall be limited only to authorized personnel of the School District.

It shall be a violation of the District's policy to release confidential computerized data to any unauthorized person or agency. Any employee who releases or otherwise makes improper use of such computerized data shall be subject to disciplinary action.

However, if the computerized information sought is available under the Freedom of Information Law and can be retrieved by means of existing computer programs, the District is required to disclose such information.

Family Educational Rights and Privacy Act of 1974, 20 USC Section 1232(g)
34 CFR Part 99
Public Officers Law Section 84 et seq.

Adoption Date: November 4, 2015

/EB

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION

The School District values the protection of private information of individuals in accordance with applicable law and regulations. Further, the District is required to notify affected individuals when there has been or is reasonably believed to have been a compromise of the individual's *private information* in compliance with the Information Security Breach and Notification Act and Board policy.

a) "*Private information*" shall mean ***personal information* in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

1. Social security number;

2. Driver's license number or non-driver identification card number; or

3. Account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

"*Private information*" <u>does not include</u> publicly available information that is lawfully made available to the general public from federal, state or local government records.

**"*Personal information*" shall mean any information concerning a person which, because of name, number, symbol, mark or other identifier, can be used to identify that person.

b) "*Breach of the security of the system*" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the District. Good faith acquisition of personal information by an employee or agent of the District for the purposes of the District is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Determining if a Breach Has Occurred

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or person without valid authorization, the District may consider the following factors, among others:

a) Indications that the information is in the physical possession or control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

b) Indications that the information has been downloaded or copied; or

(Continued)

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION (Cont'd.)

c) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported;

d) System failures.

Notification Requirements

a) For any computerized data owned or licensed by the School District that includes private information, the District shall disclose any breach of the security of the system following discovery or notification of the breach to any New York State resident whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure to affected individuals shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. The District shall consult with the State Office of Information Technology Services to determine the scope of the breach and restoration measures.

b) For any computerized data maintained by the District that includes private information which the District does not own, the District shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.

The notification requirement may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The required notification shall be made after the law enforcement agency determines that such notification does not compromise the investigation.

Methods of Notification

The required notice shall be directly provided to the affected persons by one of the following methods:

a) Written notice;

b) Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and a log of each such notification is kept by the District when notifying affected persons in electronic form. However, in no case shall the District require a person to consent to accepting such notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

c) Telephone notification, provided that a log of each such notification is kept by the District when notifying affected persons by phone; or

(Continued)

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION (Cont'd.)

d) Substitute notice, if the District demonstrates to the State Attorney General that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or that the District does not have sufficient contact information. Substitute notice shall consist of **all** of the following:

1. Email notice when the District has an email address for the subject persons;

2. Conspicuous posting of the notice on the District's website page, if the District maintains one; and

3. Notification to major statewide media.

Regardless of the method by which notice is provided, the notice shall include contact information for the notifying District and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

In the event that any New York State residents are to be notified, the District shall notify the New York State Attorney General (AG), the New York State Department of State, and the New York State Office of Information Technology Services as to the timing, content and distribution of the notices and approximate number of affected persons.

In the event that more than five thousand (5,000) New York State residents are to be notified at one time, the District shall also notify consumer reporting agencies, as defined pursuant to State Technology Law Section 208, as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York State residents. A list of consumer reporting agencies shall be compiled by the State Attorney General and furnished upon request to school districts required to make a notification in accordance with State Technology Law Section 208(2), regarding notification of breach of security of the system for any computerized data owned or licensed by the District that includes private information.

State Technology Law Sections 202 and 208

Adoption Date: November 4, 2015

Parents Bill of Rights for Data Privacy and Security

The Lockport City School District is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law Section 2-d, the District wishes to inform the school community of the following:

1) A student's personally identifiable information cannot be sold or released for any commercial purposes.
2) Parents have the right to inspect and review the complete contents of their child's educational record.
3) State and federal laws protect the confidentiality of personally identifiable information. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4) A complete list of all student data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be directed to the Chief Privacy Officer via email at: CPO@mail.nysed.gov.

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Lockport City School District has entered into agreements with certain third-party contractors. Pursuant to such agreement, third-party contractors may have access to 'student data' and/or 'teacher or principal data,' as those terms are defined by law. Below, please find relevant information regarding these agreements:

For each contract the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data, the following information must be included:

1) The exclusive purposes for which the student data or teacher or principal data will be used.
2) How the third-party contractor will ensure that the subcontractor, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, and will abide by the data protection and security requirements.
3) When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement.

4) If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected.
5) Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.