SUBJECT: OPERATION AND USE OF SECURITY SYSTEMS / PRIVACY PROTECTIONS

Scope

The Board of Education is responsible for protecting the overall safety and welfare of the District's students, staff, properties, and visitors as well as deter theft, violence and other criminal activity on District property. The purpose of this policy is to establish parameters for the operation of security systems and protection of privacy. In order to further this purpose, the Board has authorized the implementation of security systems, including, but not limited to the Raptor visitor management system, DS Control Point for the District's CCTV security cameras, and the AEGIS object and facial recognition system. The Board further recognizes the importance of safeguarding privacy consistent with law with respect to the operation and use of these security systems for the safety and protection of our school community. In no event shall a District student be placed in the AEGIS system database.

Hardware and Software

Security cameras are only placed in public or common areas, such as building entrances, stairwells, hallways, cafeterias, parking lots, auditoriums, gymnasiums or playgrounds, and not in private areas such as locker rooms, bathrooms, or other similar areas in which the District recognizes that individuals have a reasonable expectation of privacy, or in classrooms. The District will annually notify District parents that security cameras are being utilized on District property for this purpose and in the manner set forth in this Policy.

Access to Hardware Systems

Security data is protected in several ways. Hardware systems stored in the District are protected with access controls to data closets by a fob system that limits access and tracks entry. A second level of security will limit access to the hardware rack. School building Head Custodians will have access to the closet for emergency situations but not access to the rack where the security hardware is stored. Those with authorized access to security hardware systems may include the following titles, as well as any other individual specifically designated for this purpose by the Superintendent of Schools (with notice to the Board of Education President):

Director of Technology, Data Security, and Communications
Technology Supervisor
Director of Facilities

SUBJECT: OPERATION AND USE OF SECURITY SYSTEMS/PRIVACY PROTECTIONS (con't)

Access to Security System Databases

The security systems hardware and software are protected in order to maintain the safety, privacy and integrity of those systems. Password protected access to any database system used for security is limited to only the following critical staff members, as well as any other staff member specifically designated for that purpose by the Superintendent of Schools (with notice to the Board of Education President):

Assistant Superintendent for Personnel
Director of Technology, Data Security, and Communications
Director of Facilities

These individuals are identified as system administrators with the highest security privileges and the ability to access the security system databases consistent with this policy. All District officers and staff who are provided access to security hardware systems and databases pursuant to this Policy shall receive training as determined by the Superintendent of Schools and/or as required by law.

Security Alerts and Response

Security alerts may be issued when our security systems recognize a potential threat to the school community. There may also be additional communication to identified staff through the use of telephone, text, email, radio or other means as necessary. Security alerts generated from the AEGIS system will be verified by control room security officers before being issued to identified staff. When security alerts are issued, the information that is communicated is also protected and accessible to only the following staff members who are trained to confirm and respond, as well as any other staff member specifically designated for this purpose by the Superintendent of Schools.

Superintendent of Schools
Board of Education President
Assistant Superintendent for Personnel
Director of Technology, Data Security, and Communications
Technology Supervisor
Director of Facilities
District Safety Officer
Building Administrators for Alerts at Building of Responsibility (this may include Substitute administrators and main office secretarial staff as needed for alerts from the Raptor visitor management system)
School Monitors

SUBJECT: OPERATION AND USE OF SECURITY SYSTEMS/PRIVACY PROTECTIONS (con't)

The Director of Technology, Data Security, and Communications shall implement controls, such as encryption, to ensure the security of alert communications.

If a security alert is generated as a result of misidentification of a student, no record of such alert shall be maintained as part of the misidentified student's educational record, although the alert record shall be otherwise maintained by the District solely for purposes of continuing audit and review of security system operation.

The sole data to be generated and/or maintained by the security system as a result of a security alert shall be limited to the individual's name, category under this policy (as listed in the maintenance of databases section), the individual's database photo, camera image, date and time of an alert confirmation, the camera location, risk level, and the status of the alert.

Maintenance of Databases

The input and maintenance of personally identifiable information in the District's security systems will be limited to the following individuals:

(a) Staff who have been suspended and/or are on administrative leave,
(b) Level 2 or 3 sex offenders,
(c) Anyone prohibited from entry to District property by court order presented to the District,
(d) Anyone believed to pose a threat based on credible information presented to the District and
(e) School security and law enforcement personnel.

(For this purpose, a "threat" shall be limited to a threat that is referred to the District by law enforcement authorities, or a threat that, given its nature, has been or will be referred by the District to law enforcement authorities). The Superintendent of Schools (or designee if the Superintendent is unavailable and there is a credible immediate threat) will make the final determination of who belongs in the security databases used by systems such as AEGIS and Raptor consistent with this Policy. The Board of Education will be notified in the weekly update when a staff member is added to the database. "Credible information" for purposes of this Policy shall be defined as information disclosed or obtained by the District that, considering the source and nature of the information and the totality of the circumstances, is sufficiently believable to lead the District to presume that the fact or facts in question are likely true.

SUBJECT: OPERATION AND USE OF SECURITY SYSTEMS/PRIVACY PROTECTIONS (con't)

No one individual has the authority to add or remove images from the database without a directive from the Superintendent of Schools. In no event shall a District student be placed in the AEGIS system database, regardless of whether the student would otherwise fall within one of the categories set forth above.

The District will not expand the categories to be entered into the database, as specified above, except upon notification to and consultation with the Chief Privacy Officer of the New York State Education Department, and in accordance with all applicable law.

The District will notify staff who are suspended or placed on leave that their photo will be placed in the system during periods of suspension or leave. Photos will be removed once the suspension or leave has been concluded.

The Superintendent of Schools will also have the final determination regarding who is removed from security databases. Any individual requesting that a person be added or removed from the security databases must consult the Superintendent of Schools or designee in the absence of the Superintendent for a decision. Any such decision by the Superintendent or Designee may be appealed to the Board of Education.

Security databases, including personally identifiable information in the security databases used by the systems such as AEGIS and Raptor, will be audited at a minimum quarterly or more frequently as determined by administration to ensure that all images maintained in the database fall within the categories set forth in this policy, and to remove any images of individuals who no longer fall within such categories.

Any individual who believes that he or she has been improperly added to the AEGIS and/or Raptor reference database may express their concerns in writing to the Superintendent of Schools for review and determination of the Superintendent. Any such decision by the Superintendent or Designee may be appealed to the Board of Education.

Privacy

Information from security systems are maintained and used primarily to help ensure the safety and well being of the school community. In furtherance of that purpose, such information may be shared with law enforcement or other governmental authorities as required or permitted by law. The AEGIS system will not be used for student disciplinary purposes. However, only the above mentioned, select group of District employees, have access to the system and must turn over information requested as required by law or at the discretion of the Superintendent and designees.

Following the verification by a person reviewing the image in the alert, the alert is forwarded to law enforcement via the alert system.

SUBJECT: OPERATION AND USE OF SECURITY SYSTEMS/PRIVACY PROTECTIONS (con't)

The security cameras only capture images and no images collected from security systems are stored for longer than 60 days, unless the information is being evaluated or preserved as part of an investigation, or retained in conjunction with a log of confirmed security alerts. Any such retention of security system information beyond 60 days must be directed by a District-wide or building-level administrator, and must be immediately reported to the Superintendent of Schools.

The Lockport City School District does not maintain a comprehensive database of students or staff including images, demographic or any biometric data for security purposes. Images from the District's security cameras will not be linked to any other student or staff information or data except for the purposes described by this Policy.

The privacy of data and information within the District's security systems will be maintained as required by law and/or applicable District policies.

ref: 3320 Confidentiality of Computerized Information
5674 Data Network and Security Access
5680 Safety and Security
5684 Use of Surveillance Cameras in the School District and on School Buses
7241 Student Directory Information
7243 Student Data Breaches
7250 Student Privacy, Parental Access to Information and Administration of Certain Physical Examinations to Minors

Adopted: December 5, 2018
BOE Review: December 2019
BOE Review: February 27, 2019
BOE Review: August 7, 2019
BOE Review: September 18, 2019
BOE Review: January 8, 2020