Board of Education
Policy Manual

ADMINISTRATIVE REGULATION

AR 8210.01
USE OF SECURITY CAMERAS IN BUILDINGS & ON BUSES

The Burnt Hills-Ballston Lake Central School District utilizes security cameras and recognition technology to enhance the safety and security of school buildings, grounds and buses. This administrative regulation outlines the procedures and guidelines for the use of this technology.

This administrative regulation is intended to ensure that the District's use of security cameras and recognition technology is consistent with its commitment to providing a safe and secure learning environment as required by Policy 8210, while protecting the privacy rights of students and staff.

AUDIO RECORDINGS

- Audio recording capabilities in school buildings will not be used at any time. These capabilities should be turned off.
- Audio recording on school buses will be enabled. Signage will be posted on buses to remind individuals that audio and video recording is in progress.

BIOMETRIC INFORMATION COLLECTION

- The collection and monitoring of biometric information, such as facial recognition, is strictly prohibited and will be completely turned off.

PHYSICAL ATTRIBUTE RECOGNITION

- The security camera system has the capability to track physical attributes, such as clothing color or vehicle type.
- This feature may be used for specific, targeted investigations related to incidents on school property.
- Access to physical attribute recognition will be limited to authorized personnel, such as school administrators, their designees, and law enforcement at the Superintendent’s discretion.

LICENSE PLATE SCANNING

- The security camera system has the ability to scan and record license plates of vehicles on school property.
- License plate information will be used for specific, targeted purposes, such as tracking vehicles involved in accidents or incidents on campus.

- Access to license plate data will be restricted to school administrators, their designees, and law enforcement.
- License plate data will be securely stored and disposed of in accordance with the District's data retention policies.

DATA PRIVACY & SECURITY

- The District has entered into a contract with Verkada, the provider of the security camera system, through a COSER with BOCES.
- The contract includes provisions to protect the privacy and security of data collected by the system in accordance with Education Law 2-d.
- Verkada's terms and conditions acknowledge that no personally identifiable student information will be collected through the use of physical attribute recognition.

USER ACCESS TO SECURITY CAMERA FOOTAGE

- A designated location (often in the main offices) at each building will have wall-mounted viewing stations installed that display select live camera feeds from the building.
- The following staff members shall have full access to the Verkada Command system, which includes live camera access, recent historical footage, and long-term archived footage:
    - Superintendent
    - Assistant Superintendent(s)
    - Director of Technology
    - School Resource Officers

- The following staff members shall receive access to Verkada Guest & Verkada Intercom, which provides select live camera feeds from the building:
    - Main Office Secretaries
    - Executive Secretaries at the District Offices
    - Security Monitors

- The following staff members may receive access to the Verkada Command system--which includes live camera access, recent historical footage and long-term archived footage--as needed with the approval of the Superintendent:
    - Principals
    - Security Monitors
    - I.T. Manager(s)
    - Administrator for Student Transportation
    - Transportation Assistant(s)
    - Director(s) of Human Resource
    - Director of Special Education
    - Assistant Director of Special Education
    - School Resource Officers
    - Facilities Directors and Managers
    - Elementary Administrative Assistants

STAFF TRAINING & RESPONSIBILITIES

- All staff members with access to the security camera system and recognition technology will receive training on the proper use of these tools and the importance of protecting individual privacy.
- Staff will be responsible for ensuring that recognition technology is used only for specific, authorized purposes and that data is securely maintained and properly disposed of.

SANCTIONS

- Violations of this policy will be dealt with in accordance with applicable District policies and procedures. Failure to comply may result in sanctions relating to the individual's employment (up to and including termination), civil or criminal liability, or any combination of these.

ACCOUNTABILITY/ABUSE

- Any perceived misuse of the security camera system or recognition technology may be reported to the Superintendent, building principals, or the District's dignity act coordinators for review and resolution. Misuse may result in criminal, civil and administrative actions.

The Superintendent will authorize an audit of the use of the system on an annual basis to review access, inquiry logs, configuration, and to confirm active individual accounts.

Adopted January 2025