Burnt Hills-Ballston Lake
CENTRAL SCHOOL DISTRICT

Board of Education Policy Exhibit 8635

PARENTS' BILL OF RIGHTS FOR STUDENT DATA PRIVACY & SECURITY

The Burnt Hills-Ballston Lake Central School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. The Burnt Hills-Ballston Lake Central School District establishes the following parental bill of rights:

STUDENT PII

Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law. Specifically, parents are assured:

- that it is the district's policy to disclose personally identifiable information from student records, without consent, to other school officials within the district whom the district has determined to have legitimate educational interests. The notice will define 'school official' and 'legitimate educational interest.'

District policy P5500 provides the following definitions:

  - *Legitimate Educational Interest:* a school official has a legitimate educational interest if they need to review a student's record in order to fulfill their professional responsibilities;
  - *School Official*: a person who has a legitimate educational interest in a student record who is employed by the district as an administrator, supervisor, instructor or support staff member (including health or medical staff and law enforcement unit personnel); a member of the Board of Education; a person or company with whom the district has contracted to perform a special task (such as attorney, auditor, medical consultant or therapist); or a parent or student serving on an official committee, such as disciplinary or grievance committee, or assisting another school official performing their tasks.

- that, upon request, the district will disclose education records without consent to officials of another school district in which a student seeks to or intends to enroll or is actually enrolled.
- that personally identifiable information will be released to third party authorized representatives for the purposes of educational program audit, evaluation, enforcement or compliance purposes.

- that the district, at its discretion, releases directory information (see P5500) without prior consent, unless the parent/guardian or eligible student has exercised their right to prohibit release of the information without prior written consent. The district will not sell directory information.

- that, upon request, the district will disclose a high school student's name, address and telephone number to military recruiters and institutions of higher learning unless the parent or secondary school student exercises their right to prohibit release of the information without prior written consent.

- that the district will provide information as a supplement to the 'Parents' Bill of Rights' about third parties with which the district contracts that use or have access to personally identifiable student data.

- that a student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by the district or any third party contractor. The district will not sell students' personally identifiable information. The district will not release it for marketing or commercial purposes, other than directory information released by the district in accordance with district policy;

PARENTS RIGHTS

Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see AR5500); Parents have the right to request that records be amended to ensure that they are not inaccurate, misleading, or otherwise in violation of the student's privacy rights;

- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. Specifically,
    - Parents have the right to consent to disclosure of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent; and

    - Parents have the right to file a complaint with the United States Department of Education alleging failure of the district to comply with FERPA and its regulations; and/or file a complaint regarding a possible data breach by a third party contractor with the district and/or the New York State Education Department's Chief Privacy Officer for failure to comply with state law.

- 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;

- A complete list of all student data elements collected by the State Education Department is available for public review or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to the district's Data Protection Officer. Complaints can also be directed to the New York State Education Department by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to Privacy@nysed.gov or by telephone at 518-474-0937.

- Parents have the right to be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.
- Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.
- In the event that the District engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting the district's Data Protection Officer (see www.bhbl.org).
- In the course of complying with its obligations under the law and providing educational services to District residents, the Burnt Hills-Ballston Lake Central School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation. For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included in the contract and published on the District Web Page:
    - The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
    - How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);
    - The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
    - 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;
    - Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
    - Address how the data will be protected using encryption while in motion and at rest.

Email address changed July 2022 | Adopted June 2020