

# **Bronx Charter School for Better Learning Data Use, Security, and Privacy Policies**

Revised July 23, 2025



## Table of Contents

<b>Introduction</b>	<b>3</b>
“Educational Records” and “Personally Identifiable Information”	3
Acceptable Use and Disclosure of Personally Identifiable Information	4
Publishing and Annual Review of this Policy	5
<b>Family Education Rights and Privacy Act (“FERPA”)</b>	<b>5</b>
Right to be Informed of the Rights under FERPA	5
Right to Inspect and Review the Student’s Education Records	6
Right to Challenge and Request to Amend Student’s Education Records	6
Right to File a Complaint	8
<b>Data Privacy and Security Standards</b>	<b>8</b>
Staff Roles in Data Use, Security, and Privacy	9
Parents’ Bill of Rights for Data Privacy and Security	9
Third-Party Contractors	12
Procedure for Entering a Contract with Third Party Vendors	13
Third Party Reports and Notification Of Breach	13
Complaint of Breach or Unauthorized Release of Data	14
Retention Policy	15
Annual Data Privacy and Security Training	15
Practical Considerations	<b>15</b>
<b>Additional Policies</b>	<b>16</b>
<b>Appendix A: Definitions</b>	<b>18</b>
<b>Appendix B: Industry Standards for Protecting Personally Identifiable Data</b>	<b>20</b>

# Introduction

The following policies guide the BBL Network in ensuring appropriate protection of students' data. This document outlines acceptable and prohibited activities for all categories of authorized data users (teachers, administrators, researchers, etc.). These policies will define and clarify acceptable data use, define staff access, and outline compliance monitoring procedures along with consequences for noncompliance. These policies have been adopted in accordance with federal and state guidelines and regulations, including Education Law 2-d; [FERPA](#), [IDEA](#), [COPPA](#), [PPRA](#) the recent [Part 121 Strengthening Data Privacy and Security in NY State Educational Agencies to Protect Personally Identifiable Information](#) adopted by NYSED on January 13, 2020. -

## “Educational Records” and “Personally Identifiable Information”

To satisfy their responsibilities regarding the provision of education to students in pre-kindergarten through grade twelve, educational agencies in the State of New York collect and maintain certain personally identifiable information from the education records of their students. For students, personally identifiable information is information maintained in education records which can be used to identify the student with reasonable certainty, either directly or indirectly. personally identifiable information includes, but is not limited to:

- the student's name.
- the name of the student's parent or other family members.
- the address of the student or student's family.
- a personal identifier, such as the student's social security number, student number, or biometric record; or
- other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name.

For teachers and principals, personally identifiable information (personally identifiable information) includes information from the records of an educational agency, such as BBL, relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

An educational record is “any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.” (34 C.F.R. §99.3.) Education Record means those records that are:

- Directly related to the student
- Maintained by an educational agency, such as BBL, or institution

Educational records have personally identifiable information, and include, but are not limited to:

- Documents and forms related to the lottery and enrollment
- Documents related to medical information (i.e., allergies, immunization, health forms, medical 504s, athletic program release)
- Student demographic information stored electronically or in databases (i.e., race, ethnicity, lunch status, ELL, special education)
- Forms completed by and or signed by parents (i.e., field trip, receipt of report card, promotion in doubt, lunch forms)

- Student rosters (i.e., class lists, attendance forms, emergency contact lists, gradebook information)
- Records related to special education (i.e., rosters, recommendation forms, IEP, review meetings, services, records from service providers, 504s)
- Records related to English language learners (i.e., rosters, recommendation forms, evaluations, services)
- Records related to academic intervention (i.e., rosters, recommendation forms, intervention plans)
- Academic records (i.e., electronic or paper gradebooks, student work, assessment results, honor roll lists, awards)
- Behavioral records (i.e., electronic or paper anecdotal records, behavior contracts, suspensions (including reports, hearings, etc.), expulsions (including reports, hearings, etc.))
- Attendance records (i.e., days/periods students attended/did not attend, information stored electronically or on paper, early release and late arrival information)
- Photographs of students (see policies about media release)
- Student identifiable email
- Videos of students (including those taken by security cameras)
- Records related to participation in extracurricular activities
- High school application records (i.e., recommendations, applications, acceptance, final decisions)
- Transportation records (i.e., bus stop information, address, eligibility, receipt of MetroCard)
- There are other records that the school keeps that are not part of the Educational Record, but nonetheless are maintained by the school
- The National School Lunch Act (NSLA), administered by the U.S. Department of Agriculture, provides free or reduced-price meals for eligible students. It strictly limits how school districts may use individual student and household information obtained as part of the eligibility process or once students are identified to receive program services. The act ensures that neither eligibility nor program identification information may be incorporated into a student's education record. Furthermore, the statute establishes criminal penalties for unauthorized disclosures and improper use of individual school lunch eligibility or enrollment information.

### **Acceptable Use and Disclosure of Personally Identifiable Information**

Every use and disclosure of personally identifiable information by BBL shall benefit students and the school (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations).

Personally identifiable information will never be included in public reports or other documents.

BBL's data security and privacy policy will include all the protections afforded to parents or eligible students, where applicable, under FERPA and the Individuals with Disabilities Education Act (20 U.S.C. 1400 et seq.), and the federal regulations implementing such statutes.

No BBL employee may sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

BBL will take steps to minimize the collection, processing and transmission of personally identifiable information. As much as possible, BBL will rely on a small number of centralized databases to collect personally identifiable information and has sought out third-party vendors that integrate with these systems whenever possible.

BBL will ensure that it has provisions in its contracts with third party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher, or principal data maintained in accordance with federal and state law and the educational agency's data security and privacy policy. This is explained in detail later in this policy.

Except as required by law or in the case of educational enrollment data, BBL will not report to the department the following student data elements: juvenile delinquency records; criminal records; medical and health records; and student biometric information.

### **Publishing and Annual Review of this Policy**

In accordance with state law, this BBL Data Use, Security & Privacy Policy must be published by October 1, 2020. It must be placed on the school's website and notification must be provided to all officers and staff. This policy will be reviewed and updated as needed to ensure it meets the needs of federal and state regulations, and at minimum, on an annual basis.

## **Family Education Rights and Privacy Act (“FERPA”)**

The Family Educational Rights and Privacy Act (FERPA) is a federal law that affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over and consent to the disclosure of personally identifiable information from the education records. When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student (“eligible student”). The FERPA statute is found at 20 U.S.C. § 1232g and the FERPA regulations are found at 34 CFR Part 99.

FERPA provides families with a right of privacy, though this is not an absolute right and has certain limitations. Parents, and some eligible students have the:

- the right to be informed by the school of the rights accorded parents under FERPA.
- the right to inspect and review the student's education records maintained by the school(s) the child attends or has attended.
- the right to challenge and request that the school amend any portion of the student's education records that is inaccurate, misleading, or otherwise in violation of the student's privacy rights.
- the right to require the school to obtain written consent prior to the disclosure of personally identifiable information, except in those instances specifically allowed for by law.
- the right to file a complaint with the Family Policy Compliance Office of the United States Department of Education alleging a denial of rights.

### **Right to be Informed of the Rights under FERPA**

Parents/guardians are informed of their rights by the school of their rights under FERPA in each school's annual Parent-Student Handbook. The handbook also includes instructions for accessing the full policy in this parent-facing document.

### **Right to Inspect and Review the Student's Education Records**

Parents/guardians have the right to inspect and review the student's education record maintained by the school(s) the child attends or has attended by making a request directly to BBL in a manner prescribed by the BBL.

At BBL, the procedure for parents/guardians to exercise this right includes:

- Parents/guardians must complete the following form and submit to the school to exercise this right. In accordance with Education Law Section 2-D Part 121 and FERPA, BBL requires that requests to inspect and review education records be made in writing.
- This form will then be given to one of the Data Protection Specialists (Data Liaison and IT Specialists)
- The school verifies the identity of the person who completed the request to ensure that they are a parent, or eligible students authorized to make the request.
- The school must provide access to the student record, within a reasonable period, but not more than 45 calendar days after receipt of a request
- The school should not under any circumstances provide information that includes personally identifiable information for other students.
- The schools must maintain a log of each request for access and each disclosure of "Personally Identifiable Information." The parent or eligible student is entitled to inspect this log.
- Access to the educational record may be given digitally if the parent consents to this.

Additionally, requests by a parent or eligible student for access to a student's education records must be directed to the school and not to a third-party contractor.

### **Right to Challenge and Request to Amend Student's Education Records**

Parents/guardians also have the right to challenge and request that the school amend any portion of the student's education records that is inaccurate, misleading, or otherwise in violation of the student's privacy rights.

Under FERPA, a school must provide the parent with an opportunity to inspect and review their students education records within 45 days following its receipt of a request.

The procedure by which parents can challenge or request the school amend a portion of the student's record is as follows:

- A parent can request the school principal to amend an inaccurate, misleading record or otherwise violate the student's privacy rights in writing by submitting the Request to Amend Record to the School's Principal and the Data Protection Specialist, specifying why the record is inaccurate.
- The School Data Protection Specialist within two (2) days will submit the Request to Amend Record form to the BBL School Principal with a copy to the BBL Chief Privacy Officer.
- The School Data Protection Specialist will log this request onto the "Request to Amend Record form" link

- The BBL School Principal will review the Parent's Request to Amend Record and specific records, which will include an investigation with the school leader, and render a decision within 45 days from the date of receiving the parent request
- The BBL School Principal will inform the BBL Chief Privacy Officer of the Principal's investigation and decision of whether to amend the record.
- The BBL Chief Privacy Officer will notify the parents of the decision in writing.
- If the BBL Chief Privacy Officer denies the request to amend the record, he/she will advise the parent in writing their right to a hearing regarding the denial of a record amendment.
- Additional information regarding the hearing procedures will be provided to the parents when notified of the right to a hearing.

The procedure by which parents can request a hearing if BBL decides not to amend the record as requested:

- Parents will be notified in writing that BBL decides not to amend the record as requested and informs the parent of their right to request a hearing in writing on this matter.
- BBL upon receiving written requests from parents will schedule a hearing to hear the parents request to challenge the decision not to amend the content of the student's education records on the grounds that the information contained in the education records is inaccurate, misleading or in violation of the privacy rights of the students
- BBL shall give the parents in writing the notice of hearing date, time and place.
- The parents shall have a full and fair opportunity to present evidence relevant to the issues raised.
- The parent at their own expense may be assisted or represented by one or more individuals of his/her own choice including an attorney
- If as a result of the hearing, the CEO, or their designee, decides that the information is inaccurate, misleading or otherwise in violation of the privacy rights of the student, the school shall:
  - Amend the record; accordingly, and:
  - Inform the parent or eligible student of the amendment in writing.
- If as a result of the hearing, the CEO, or their designee, decides that the information in the education record is not inaccurate, misleading, or otherwise in violation of the privacy rights of the student, BBL shall inform the parent of the right to place a statement in the record commenting on the contested information in the record or stating why he/she disagrees with the decision of BBL
- If BBL places a statement in the education records of the student, BBL shall be maintain the statement with the contested part of the record for as long as the record is maintained
- Disclose the statement whenever it discloses the portion of the record to which the statement relates

Schools are permitted to disclose records without parental consent with school officials. School officials may include an outside contractor, consultant, volunteer, or other party to whom an agency or institution has outsourced institutional services or functions if the individual:

- Performs an institutional service or function that would otherwise be performed by an employee.
- It is under the direct control of the school with respect to the use and maintenance of education records; and
- It is subject to FERPA's rules regarding re-disclosure of personally identifiable information from education records. (Education Law § 2-d and 8 NYCRR Part 121)

- Imposes an obligation on the State Education Department to take action to provide guidance on strengthening data privacy and security
- Protects student data and teacher and principal data

Schools must maintain a log of each disclosure of “Personally Identifiable Information.” There will be a log for each individual student and a log for disclosure grade or schoolwide data (such as to a third-party vendor) that will be created and maintained by Data Protection Specialists (Data Liaison and IT Specialists) at each school. The parent or eligible student is entitled to inspect this log. This includes allowable disclosure that does not require parental consent.

Parents/Guardians have the right to require the school to obtain written consent prior to the disclosure of personally identifiable information, except in those instances specifically allowed for by law. Here, "disclose" or "disclosure" means to permit access to, or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic, whether intended or unintended. (8 NYCRR Part 121 and 34 C.F.R. 99.3).

FERPA requires that a “parent or eligible student shall provide a signed and dated written consent before an educational agency or institution discloses personally identifiable information from the student’s education records” (34 C.F.R. § 99.30(a); see also 20 U.S.C. §1232g(b)(1)). Generally, schools must have consent to disclose information from an educational record, except as described above.

Under certain circumstances, records and information may be disclosed without consent.

### **Right to File a Complaint**

The right to file a complaint with the Family Policy Compliance Office of the United States Department of Education alleging a denial of rights. The address for these complaints is:

Family Policy Compliance Office  
 US Department of Education  
 400 Maryland Avenue, SW  
 Washington, DC 20202-4605

This process is outlined for families in the full policy,

## **Section 2-D: Unauthorized Release of PII - Data Privacy and Security Standards**

Under Education Law §2-d, BBL is required to adopt technologies, safeguards, and practices that align with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (“NIST”). BBL must protect Personally Identifiable Information (personally identifiable information) by:

- Ensuring that use and disclosure of personally identifiable information benefits students
- Prohibiting the inclusion of personally identifiable information in public reports or other public documents

- Using industry standard safeguards and best practices, such as encryption, firewalls, and passwords

### **Staff Roles in Data Use, Security, and Privacy**

At the state level, the Commissioner of Education appointed a Chief Privacy Officer who will report to the Commissioner on matters affecting privacy and security of student data and teacher and principal data. Every school must report breaches or unauthorized releases of student data or teacher or principal data to the Chief Privacy Officer. The Chief Privacy Officer has the power to:

- Access records maintained by the school related to student data or teacher or principal data
- Require schools to ensure that personally identifiable information is protected by requiring the performance of a privacy impact and security risk assessment
- Investigate reports or breaches, including those by third party contractors

As required by NYSED, BB has designated an employee to serve as a Network **Data Protection Officer** to serve as the main point of contact for the school's data privacy and security. At BBL, this individual will be the Network IT Manager. This person must have knowledge, training and experience to administer this role. The Data Protection Officer's responsibilities include:

- The implementation and oversight of data privacy and security procedures
- Annually report to the Board on data privacy and security activities, including a summary of complaints about breaches
- Report breaches of student, principal, or teacher data to the Chief Privacy Officer
- Ensuring that all school-based and network-based staff understand the policies in this guide and to ensure that there is an annual training of staff in this policy

At each individual BBL school, the IT Specialists and Data Liaisons will serve as School **Data Protection Specialists** who will ensure that at a school level all procedures are in place. These two roles will work together to ensure:

- Work closely with the school leadership to ensure the implementation of these protocols and procedures around data
- Regularly report on the implementations of these protocols and procedures to the Data Protection Officer

All other staff are responsible for understanding the policies in this guide and how it impacts their own work, specifically how they handle personally identifiable information. They will understand the roles of the Data Protection Officer and Data Protection Specialists.

### **Parents' Bill of Rights for Data Privacy and Security**

Education Law §2-d requires that BBL develop a Parents' Bill of Rights for Data Privacy and Security (Parents' Bill of Rights). The purpose of the Parents' Bill of Rights is to inform parents (which also include legal guardians or persons in parental relations to a student, but generally not the parents of a student who is age eighteen or over) of the legal requirements regarding privacy, security and use of student data. In addition to the federal Family Educational Rights and Privacy Act (FERPA), Education Law §2-d provides important new protection for student data, and new remedies for breaches of the responsibility to maintain the security and confidentiality of such data.

The BBL Network will ensure that the Parent's Bill of Rights for Data Privacy and Security is:

- published on its website; and
- included with every contract it enters with a third-party contractor where the contractor will receive student data or teacher or principal data.

### **BBL Parent's Bill of Rights for Data Privacy and Security**

Bronx Charter School of Better Learning (BBL) and its schools are responsible for providing parents (which also include legal guardians or persons in parental relation to a student) with access to their child's education records and any available information on educational programs and opportunities. Parents have the right to:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and FERPA, includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including but not limited to encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at [www.nysed.gov/data-privacy-security](http://www.nysed.gov/data-privacy-security), and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. Complaints may be submitted to NYSED at [www.nysed.gov/data-privacy-security](http://www.nysed.gov/data-privacy-security); by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to [privacy@nysed.gov](mailto:privacy@nysed.gov); or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

## Entering into Contracts with Third-Party Contractors

A third-party contractor means “any person or entity, other than an education agency that received student data or teacher or principal data from BBL pursuant to a contract or other written agreement for purposes of providing services to BBL including but not limited to data management or storage services, conducting studies for or on behalf of BBL , or audit or evaluation of publicly funded programs. This term will include an educational partnership organization that receives student and/or teacher or principal data from a school to carry out its responsibilities pursuant to Education Law Section 211-e and is not an educational agency, and a not-for-profit corporation or other nonprofit organization, other than an educational agency.” (8 NYCRR 121.1(s))

The Supplement to Bill of Rights for every third-party contractor that will receive personally identifiable information must be published on the website. Information may be redacted to the extent necessary to safeguard the privacy of the data.

The Data Privacy Officer will create this supplement to the Bill of Rights whenever new third-party contracts are developed or if existing contracts are modified using this. Checklist for 3rd Party Contracts related to Data and Security

Each contract with a third-party contractor receiving personally identifiable information must include provisions requiring the confidentiality of personally identifiable information be maintained in accordance with federal and state laws, regulations, and the school’s policy. The contract must include a Data Privacy and Security Plan, which must:

- Outline how data privacy and security contract requirements over the life of the contract will be implemented
- Specify how officers or employees and assignees who have access to student data or teacher or principal data receive or will receive training on the federal and state laws and regulations governing confidentiality of this data prior to receiving access
- Specify if subcontractors will be used and how it will manage those relationships and contracts to ensure personally identifiable information is protected o Specify how the data privacy and security incidents that implicate personally identifiable information will be managed including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the school
- Include language how the Parent’s Bill of Rights will be followed.
- Include signed Parent’s Bill of Rights as addendum to the contract.
- Include language of duration of contract /written agreement with beginning and expiration dates.
- Describe how data will be destroyed upon expiration of the contract
- Comply with the school’s data security and privacy policy, Federal and State regulations including Ed. Law 2-d. And Part 121.
- Include a clause that they will not sell student (teacher or principal) data and use the data for any marketing or commercial purpose
- Explain how third-party contractors will ensure that subcontractors or other authorized entities that will have access to data will abide by all applicable data protection and security requirements

- Explain If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of data collected
- Address how the data will be protected using password protections, administrative procedures, encryption, and firewalls
- Include a clause that parents will be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their students Personal Identifiable Information (PII) occurs Be assured that State and federal laws such as NYS Education Law 2-4 and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, are in place when data is stored or transferred
- Indicate clause for "No disclosure of information to any other party without prior written consent, unless required by statute or court order or party is an authorized representative of third-party contractor"
- Include clause that they "Shall promptly notify the school of any breach of Personally Identifiable Information without reasonable delay but no more than seven (7) calendar days of any breaches or unauthorized release of PII data of when the breach occurred.
- Shall promptly notify the school of any breach of Personally Identifiable Information without reasonable delay but no more than seven (7) calendar days of any breaches or unauthorized release of PII data of when the breach occurred.
- Third party contractors must cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.
- Not disclose information to any other party without prior written consent or eligible student, unless required by statute or court order or party is an authorized representative of third-party contractor.
- Include Hold Harmless/Indemnification clause indicating the 3rd party contractor agrees to defend, indemnify, and hold harmless The Bronx Charter School of Better Learning ols for all losses, costs and expenses arising out of their negligence.
- Carry General Liability Insurance as required by law and Employers' liability with limits of \$1,000,000, waiving insurer's right of subrogation against The Bronx Charter School of Better Learning ols.

When any BBL school, or the schools as a network, are looking to contract with a third-party vendor with which it will share student data, the contract must be reviewed by the Data Protection Officer and F Finance Office. It is the joint responsibility of school-based Data Protection Specialists and the School leadership to ensure that these contracts have been shared with both the Data Protection Officer and Finance Office.

Upon receiving a potential contact, the Data Protection Officer will:

- Use the checklist to ensure that the contracts meet the requirements as stated above
- Contact the contractor to receive an assurance for any item not in the contract
- Ensure that it includes a signed copy of the Parent's Bill of Rights for Data Privacy and Security
- Include Insurance Requirements for 3rd Party Contractor

### **Third Party Reports and Notification Of Breach**

If a third-party contractor discovers a breach or unauthorized release, it must immediately notify the school in the most expedient way, but no more than 7 days after the discovery; and cooperate with law enforcement and the school during the investigation.

The BBL Data Protection Officer must notify the Chief Privacy Officer, as designated by SED, within 10 days of the reported breach by the third-party contractor. Every discovery or report thereafter must also be sent to the Chief Privacy Officer within 10 days.

Parents, eligible students, teachers, principals and other staff of the affected BBL school(s) must be notified by the school of any discovered breach within 60 calendar days unless the breach interferes with ongoing law enforcement investigation or causes further disclosure of personally identifiable information. Notification must be provided within 7 calendar days after security vulnerability remedied or risk of interference with law enforcement investigation ends. The school should seek reimbursement for any expenses incurred in notification from the third-party vendor, who is obligated to pay for these expenses.

Notification to parents, eligible students, teachers, principals and other staff of an educational agency must be clear and concise, and must include:

- A brief description of the breach.
- The dates of the incident and date of discovery.
- A description of the types of personally identifiable information that were affected.
- An estimated number of affected records.
- A brief description of the school's investigation or investigation plan; and
- Contact information of the Data Protection Officer who can assist parents or eligible students who have additional questions.
- Notification sent by first class mail to last known address, by email, or by telephone

A template for notification of a data breach can be found [here](#).

### **Complaint of Breach or Unauthorized Release of Data**

In the event of a complaint about breaches and unauthorized release of personally identifiable information, the following procedure should be enacted:

1. Complaints must be submitted to the Data Protection Officer in writing.
2. BBL Data Privacy Officer will promptly acknowledge receipt of the complaint to the complainant via email within three (3) days of notification
3. Third-party contractors must inform the BBL Data Protection Officer of a breach no more than seven (7) calendar days of the occurrence of the breach.
4. The BBL Data Privacy Officer will inform the NYSED Chief Privacy officer no more than 10 Days from the date of the breach.
5. The BBL Data Privacy Officer will commence an investigation and take the necessary precautions to protect personally identifiable information.

6. Following its investigation of a submitted complaint, BBL shall provide the parent or eligible student, teacher, principal or any other staff member of BBL who filed a complaint with its findings within a reasonable period but no more than 60 calendar days from the receipt of the complaint by BBL. Where BBL requires additional time, or where the response may compromise security or impede a law enforcement investigation, BBL shall provide the parent eligible student, teacher, principal or any other staff member of BBL who filed a complaint with a written explanation that includes the approximate date when BBL anticipates that it will respond to the complaint.
7. BBL , through the Data Privacy Officer will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004), as set forth in section 185.12, Appendix I of this Title.

This complaint policy will be communicated to parents, eligible students, teachers, principals or other staff through the school website.

### **Retention Policy**

Schools are required to maintain a record of all complaints of breaches or unauthorized release and its disposition in accordance with data retention policies pursuant to Education Law §185.12. o §185.12 – ED-1 has not updated its Records Retention Schedule to specifically include the retention of complaints pursuant to §2-d. A 6 year minimum is required for general complaints.

### **Annual Data Privacy and Security Training**

Annual privacy and security awareness training is required for all officers and employees with access to personally identifiable information. This training must include but is not limited to: training on the state and federal laws that protect personally identifiable information and how employees can comply with such laws.

BBL has prepared an internal self-paced training and certification form for staff to complete on an annual basis.

## **Adopting New Programs: A Checklist for School Staff**

In the adoption of this policy and to be in compliance with state regulations, each BBL school has

- Compiled a list of programs being used by the school or school staff that receive student, teacher or principal data
- Ensure that there are agreements that include the required elements with each vendor
- Ensure that these supplemental agreements are posted to the website
- Ensure that any data transfers to these vendors is done according to industry standards and best practices, including but not limited to encryption, firewalls, and password protection
- Ensure that all staff are informed that physical PII records to be disposed of are shredded.

In the future, any time that a school wishes to adopt a program that receives student, teacher, or principal data, the school must first consult with the Data Privacy Officer, who will complete the

necessary steps to ensure that the agreements with the third-party vendor satisfy the requirements under and are posted in accordance with Part 121. When new programs or technological options for use in classroom or remote settings are being considered:

- The schools must consult with the Data Protection Officer in school for information for technology options available and supported for use in the classroom or remote settings.
- The Data Protection Officer will send confirmation to the schools via email of the suitability of the resource or program in light of the policies in this document.
- The Data Protection Officer will enter into an Education Law 2-d agreement with a municipal corporation that has licenses with vendors of choice
- The Data Protection Officer will adopt industry standards and best practices, including but not limited to encryption, firewalls, and password protection when data is stored or transferred and communicate how data may be transferred between this third-party and the school
- Any time that data needs to be transferred, this process must be overseen by either the Data Privacy Officer or by the IT Specialists at the school, who will be trained by and report to for this purpose, the Data Privacy Officer.

## **Additional Policies**

### **Data Reporting to Entities Outside of the Organization**

BBL will not disclose student level data when sharing reports on academic or other progress with outside entities, including the Board of Trustees, except as required by the state and federal entities.

In sharing data, data will always be presented without personally identifiable information. In the event that the number of students in a category of data presented is less than 5 students, the data for this group will be suppressed. Additionally, if the category suppressed is a subgroup of a larger group that is also presented, the data of the next smallest subgroup will also be suppressed. (For example, if the test scores of third graders is presented, and the subgroup data for rac/ethnicity is presented, the data from any subgroup with fewer than 5 students will be suppressed, as will the next smallest subgroup as this data could be extrapolated from the data on all third graders.) This done so as not to inadvertently disclose student level data.

### **Student Data Record Retention of Sub-Contractor**

The Laws of 2008 (Chapter 8) effectively revised Section 220 (3-a) of the Labor Law upon which the retention and disposition of this contractor records item was based. The revised law lengthens the retention period of contractor records to five years after contract completion. To avoid premature destruction of these records, education officials should cease destroying records as authorized by the relevant item and should instead follow the indicated retention period prescribed by law and by the proposed new item below. The New York State Archives intends to revise this item in future editions of the Schedule ED-1. The proposed revision of the item is as follows: [ ] Records filed by contractor or sub-contractor with local government related to public works project, pursuant to Section 220 (3-a), Labor Law, including but not limited to copy or abstract of payroll, classification of workers employed on a project, and statement of work to be performed by each classification: RETENTION: 5 years after contract completion

## Appendix A: Definitions

These definitions come from Part 121, Strengthening Data Privacy and Security in NY State Educational Agencies to Protect Personally Identifiable Information. The following terms shall have the following meanings:

**Biometric record** as used in the definition of *personally identifiable information*, means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.

**Breach** means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.

**Chief Privacy Officer** means the Chief Privacy Officer appointed by the Commissioner pursuant to Education Law §2-d.

**Commercial or Marketing Purpose** means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve or market products or services to students.

**Contract or other written agreement** means a binding agreement between an educational agency and a third-party, which shall include but not be limited to an agreement created in electronic form and signed with an electronic or digital signature or a click wrap agreement that is used with software licenses, downloaded and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.

**Disclose or Disclosure** mean to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.

**Educational Agency** means a school district, board of cooperative educational services (BOCES), school, or the Department.

**Education Records** means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.

**Eligible Student** means a student who is eighteen years or older.

**Encryption** means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

**FERPA** means the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.

**NIST Cybersecurity Framework** means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 which is available at the Office of Counsel, State Education Department, State Education Building, Room 148, 89 Washington Avenue, Albany, New York 12234.

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

**Personally Identifiable Information**, as applied to student data, means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and as applied to teacher and principal data, means personally identifiable information as such term is defined in Education Law §3012-c (10).

**Release** shall have the same meaning as Disclosure or Disclose.

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

**Student Data** means personally identifiable information from the 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 Education Law §§3012-c and 3012-d.

**Third-Party Contractor** means 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 Education Law §211-e and is not an educational agency, and a not-for-profit corporation or other nonprofit organization, other than an educational agency.

**Unauthorized Disclosure or Unauthorized Release** means any disclosure or release not permitted by federal or State statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

## Appendix B: Industry Standards for Protecting Personally Identifiable Data

The following points go over different areas BBL ensures that our systems protect all PII. BBL follows best practices to secure PII based on NIST standards.

**Internal connections:** Through the Universal Service Administrative Company E-rate program BBL is partnered with IKON, who monitors all internal connections on site 24 hours a day. IKON ensures that all internal connections are encrypted and configured so that any attempts of breaches can be detected and handled appropriately.

**Note:** Internal connections are any hardware that includes but is not limited to: Managed switches, routers, Wireless access points, firewalls, and wiring.

**Firewall:** BBL employs a firewall in each school building that monitors and filters all data traffic allowed to go in and out of the building.

**System Updates:** BBL regularly ensures that all systems are up to date with the latest software which includes but is not limited to: Operating system Upgrades, anti-virus software updates, anti-malware software, and security patches.

**Cloud platforms:** BBL ensures that all cloud-based platforms are monitored by the Technology team on site to ensure there is no unauthorized use. For more information please refer to the NIST Guidelines on Security and Privacy in Public Cloud Computing