Data Privacy and Security Policy

Updated October 2025

1. Purpose and Commitment

Prospect Schools and Brooklyn Prospect Charter Schools (collectively, "Prospect Schools") are committed to protecting the confidentiality, integrity, and availability of student, teacher, and principal personally identifiable information (PII). This policy establishes administrative, technical, and physical safeguards that ensure compliance with all applicable federal and state data privacy and security laws, including:

- Family Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Act (COPPA)
- Individuals with Disabilities Education Act (IDEA)
- New York State Education Law §2-d
- 8 NYCRR Part 121

The goal of the Data Privacy and Security Policy is to promote transparency, responsible data use, and the trust of students, parents/guardians, and staff.

2. Scope

This policy applies to all employees, contractors, consultants, volunteers, and vendors who access, process, store, or transmit PII on behalf of the Prospect Schools .

3. Definitions

Key terms include:

- **Personally Identifiable Information (PII):** Any data/image/information that can directly or indirectly identify an individual.
- **Student Data:** PII from student education records as defined under FERPA.
- **Teacher or Principal Data:** PII from records related to annual professional performance reviews.
- **Breach:** Unauthorized acquisition, access, use, or disclosure of PII.
- **Third-Party Contractor:** Any outside party receiving PII through a contract or other written agreement to provide services.

(Additional definitions follow 8 NYCRR §121.1)

4. Legal Compliance

Prospect Schools will:

- Comply with FERPA, COPPA, IDEA, New York Education Law §2-d, and all other applicable laws and regulations in collecting, storing, and disclosing PII.

- Ensure that every use or disclosure of PII benefits students and the school (e.g., improving instruction, enhancing safety, or promoting efficient operations).
- Never sell PII or use it for marketing or commercial purposes.

5. Data Protection Standards

The network adopts the **National Institute of Standards and Technology (NIST) Cybersecurity Framework (Version 1.1)** as its data privacy and security standard.
Safeguards include:

- Encryption of PII in transit and at rest.
- Strong password and access control measures.
- Network firewalls, intrusion detection, and periodic vulnerability testing.
- Data minimization and secure destruction when PII is no longer needed.

6. Governance and Responsibilities

Data Protection Officer (DPO)

Prospect Schools designated Data Protection Officer (Director of IT Operations) is responsible for:

- Implementing this policy and monitoring compliance.
- Serving as the primary point of contact for data privacy and security matters.
- Coordinating with the network's legal and technology teams.

The DPO must have appropriate training and experience in privacy and cybersecurity.

Chief Privacy Officer (CPO)

The network will cooperate with the **NYSED Chief Privacy Officer** on matters involving breaches, complaints, and compliance reviews.

7. Third-Party Contractors

Under FERPA, COPPA, and N.Y. Education Law §2-d, Prospect Schools may consent to disclosing student information to authorized Third-Party Contractors providing educational services that meet certain requirements and have entered into written agreements with Prospect Schools. Third-Party Contractors must agree to comply with federal, state, and local laws, as well as Prospect School's Data Privacy and Security Policy and the Parents' Bill of Rights for Data Privacy and Security. Additional information on Data Privacy Agreements with Third-Party Contractors can be found here.

All agreements that provide a third-party with access to PII must:

1. Include a **signed Parents' Bill of Rights for Data Privacy and Security**.
2. Include a **Data Privacy and Security Plan** that:
    - Aligns with the NIST Cybersecurity Framework.
    - Details safeguards, encryption methods, and access controls.
    - Describes staff training and subcontractor oversight.
    - Requires breach notification within seven (7) calendar days of discovery.

- Specifies secure data destruction or return upon contract termination.

No software or “click-wrap” applications involving PII may be used without prior DPO approval.

8. Parents’ Bill of Rights

Prospect Schools will publish on its website a **Parents’ Bill of Rights for Data Privacy and Security**.

9. Data Access and Parental Rights

Parents/guardians and eligible students (students 18 years or older) have the right to:

- Inspect and review a student’s education record.
- Request correction of inaccurate records.
- File complaints about unauthorized data disclosures.

Requests for access must be submitted in writing and processed within **45 calendar days**.

10. Breach and Incident Response

- Any discovery of a **breach or unauthorized release** of PII must be reported to the **NYSED Chief Privacy Officer** within **10 calendar days** of discovery.
- Affected parents/guardians, eligible students, teachers, and principals must be notified **within 60 calendar days** of discovery, unless delayed for law enforcement reasons.
- Notifications must be clear, concise, and include:
  - Description and date(s) of the incident;
  - Categories of information affected;
  - Number of records impacted;
  - Contact information for further assistance.

All incidents will be logged, investigated, and remediated according to internal procedures.

11. Complaints

Parents/guardians, eligible students, teachers, or principals may file complaints about possible breaches of data privacy or security by submitting a written complaint to the school’s **Data Protection Officer** (privacy@prospectschools.org). Complaints must be acknowledged promptly, investigated, and resolved within 60 calendar days, unless additional time is needed due to law enforcement or security concerns.

12. Annual Training

All staff with access to PII must complete **annual data privacy and cybersecurity training** covering:

- FERPA, COPPA, IDEA, and N.Y. Education Law §2-d requirements;
- Safe data handling and incident reporting; and
- Recognizing phishing and social engineering risks.

13. Enforcement

Violations of this policy may result in disciplinary action, up to and including termination of employment, termination of access privileges, or referral to law enforcement or regulatory agencies, as appropriate.

14. Policy Review

This Data Protection and Security Policy will be reviewed **annually** and updated as needed to reflect changes in law, regulation, and best practices.