DATA SECURITY AND PRIVACY POLICY

1. Purpose and scope

This policy applies to Urban Dove Team Charter School I (Brooklyn South), Urban Dove Team Charter School II (Bronx), Urban Dove Team Charter School III (Queens), Urban Dove Team Charter School IV (Manhattan), and Urban Dove Team Charter School V (Brooklyn North), collectively referred to as the "Schools."

The Schools will protect the privacy, confidentiality, integrity, and availability of student information and protected teacher and principal evaluation information. This policy applies to trustees, employees, volunteers, consultants, and contractors who access or maintain covered information for any of the Schools, including central office personnel providing services to the Schools.

The Schools will comply with New York Education Law § 2-d, 8 NYCRR Part 121, the Family Educational Rights and Privacy Act (FERPA) and its regulations, and applicable Individuals with Disabilities Education Act confidentiality requirements. The policy covers paper and electronic records and information stored, transmitted, or processed by service providers.

2. Covered information and permitted use

Personally identifiable information (PII) includes information that directly identifies a student, such as a name or student number, and information that can identify a student when combined with other available information. Covered teacher and principal data means confidential annual professional performance review information protected by Education Law § 2-d.

The Schools will collect and use information only for authorized educational, operational, or legally required purposes. Student PII will not be sold or used or disclosed for commercial or marketing purposes. The Schools will not facilitate or permit another party's use or disclosure of student PII for commercial or marketing purposes. Access and disclosure require consent from the parent or eligible student unless a lawful exception applies. Information will be limited to what is necessary for the approved purpose.

Public reports will use aggregate or de-identified information and will be checked for small groups or combinations of details that could identify a student.

3. Data Protection Officer and responsibilities

Each School will designate a qualified Data Protection Officer (DPO). A shared designee may serve all Schools when formally designated for each. The DPO will coordinate compliance, privacy complaints, vendor reviews, staff training, incident response, and communication with NYSED. School Leaders and central office departments will support implementation; technology personnel will maintain technical safeguards.

Data Protection Officer for all Schools:

Michael Lukauskas, Associate Director of Data and Programming

21-21 41st Avenue, Suite 2D, Long Island City, NY 11101
info@urbandove.org
212-244-2313

The Schools will maintain a data governance team led by the DPO. The team will review proposed uses of PII to determine whether they benefit students and the Schools, including improving academic achievement, providing useful information to families and students, or supporting effective school operations. The team will oversee measures to prevent student identification in public reports and other public documents.

Employees must promptly report suspected loss, improper access, or unauthorized disclosure to the DPO and School Leader. Staff must not delay reporting while attempting to determine whether an incident is a confirmed breach.

4. Security framework and safeguards

The Schools will maintain a documented data security and privacy program aligned with the NIST Cybersecurity Framework adopted by NYSED under Part 121, including governance, identification of risks, protection, detection, response, and recovery. The program will include inventories of sensitive information, systems, and vendors; risk assessments; assigned responsibilities; and documented corrective actions.

Safeguards will include access based on job duties and legitimate educational interests; unique accounts; strong authentication and multifactor authentication where appropriate; prompt account removal after departures or role changes; encryption of covered electronic data in storage and transmission; firewalls; security updates; device protections; monitoring; secure backups; and tested recovery procedures. Paper records will be secured against unauthorized access.

Staff may use only approved systems and transfer methods for PII. Staff must not place covered data in personal accounts, unapproved cloud services, or unapproved AI tools. Security vulnerabilities, passwords, access credentials, and confidential system configurations will not be published with this policy.

5. Training and access management

The Schools will provide annual data privacy and security awareness training to officers and employees with access to PII. Training will address legal duties, approved tools, phishing, secure sharing, incident reporting, and protection of paper and electronic records. The DPO will maintain completion records. Contractors must ensure their personnel receive required training before accessing covered data.

Access will be reviewed periodically and when duties change. Users must protect credentials, lock unattended devices, verify recipients before sending records, and use secure storage and disposal methods.

6. Third-party contractors

Before a vendor receives covered data, the Schools will review its purpose, safeguards, and contractual protections. This review applies to student information systems, learning applications, assessment providers, cloud storage, and other services that receive PII. Staff may not independently authorize new data-sharing services.

Each applicable agreement must include the Parents' Bill of Rights, required supplemental information, and the third-party contractor's data security and privacy plan addressing implementation throughout the agreement. The Schools will review and accept the contractor's plan before covered data is shared. Contracts must limit data use and access to authorized purposes, bind subcontractors to applicable protections, require encryption and other safeguards,

and address training, incident reporting, cooperation, return or destruction of data, and notification costs attributable to the contractor.

Required supplements will be published for each applicable agreement. A general vendor list does not replace contract-specific disclosures. The Schools will monitor compliance and address deficiencies before continuing data sharing when necessary.

Parents' Bill of Rights for Data Privacy and Security:
https://urbandove.org/wp-content/uploads/2026/10/UDTCS-Parents-Bill-of-Rights-for-Data-Privacy-and-Security.pdf

7. Retention and secure disposal

Records will be retained according to applicable New York State records retention requirements and the Schools' adopted retention schedule. Records subject to a pending inspection request, complaint, investigation, litigation hold, or other preservation duty will not be destroyed until permitted.

When retention obligations end and the information is no longer needed, the Schools will securely destroy paper records and securely erase or destroy electronic records and media. Vendors must return or destroy data as required by their agreements and applicable law, with confirmation of disposition when required.

8. Parent and eligible student access

Parents and eligible students should submit requests to inspect and review education records in writing to the School Leader or DPO, rather than directly to a third-party contractor. The Schools will assist individuals who need help submitting a written request. Identity and authority will be verified. Access will be provided within a reasonable period, no later than 45 days after receipt of the request, and earlier when required by applicable special education rules. Copies or other arrangements will be provided when needed to make inspection possible.

If the parent or eligible student consents, the School may provide requested records electronically. Electronic delivery must comply with applicable law and use safeguards consistent with industry standards and best practices, including encryption and password protection. The School will verify the recipient and use an approved secure delivery method.

Current annual FERPA Notification of Rights:
https://urbandove.org/wp-content/uploads/2025/09/Student-and-Family-Handbook.pdf

Requests to correct inaccurate, misleading, or privacy-violating information will be considered under FERPA. If a request is denied, the School will explain the applicable hearing rights and the right to place a statement in the record following the hearing process. FERPA rights generally transfer to a student at age 18 or upon attendance at a postsecondary institution, subject to lawful exceptions.

9. Privacy complaint procedure

Parents, eligible students, teachers, principals, and other staff may submit a complaint about a possible breach or unauthorized release to the DPO by email, telephone, or mail. Include the School, contact details, the concern, approximate dates, and relevant supporting information. Do not send sensitive records through unsecured email; the DPO will arrange a secure method when needed.

Data Privacy Complaint Form: https://urbandove.org/contact/

Use of the form is encouraged but is not required to submit a complaint. Individuals may also submit a written statement or contact the DPO for assistance by telephone.

The DPO will promptly acknowledge receipt, begin an investigation, take protective measures, and maintain a record of the complaint and disposition. Findings will be provided within a reasonable period, but no more than 60 calendar days after receipt, subject to the extension procedure that follows. If additional time is required, or a response would compromise security or impede a law enforcement investigation, the Schools will provide the complainant with a written explanation and the approximate date when a response is anticipated.

Complaints may also be submitted directly to NYSED through its privacy complaint process:
https://www.nysed.gov/data-privacy-security/parents-and-students-file-privacy-complaint
Mail: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

10. Incident response and notification
The DPO will coordinate containment, preservation of evidence, assessment of affected data and individuals, investigation, recovery, and corrective action. The Schools will document decisions and cooperate with NYSED and law enforcement as appropriate.

Contractors must notify the School in the most expedient way possible and without unreasonable delay, no later than seven calendar days after discovery of a breach or unauthorized release. The Schools will report covered incidents to NYSED's Chief Privacy Officer without unreasonable delay and no later than 10 calendar days after discovery or receipt of a contractor's notice.

Affected parents, eligible students, teachers, or principals will be notified in the most expedient way possible and without unreasonable delay, but no later than 60 calendar days after discovery or receipt of a report or contractor notification of a breach or unauthorized release. Notification may be delayed only where it would interfere with an ongoing law enforcement investigation or cause further disclosure of PII by revealing an unfixed security vulnerability. Where notification is delayed for these reasons, the Schools will notify affected individuals within seven calendar days after the vulnerability is remedied or the risk of interference with the law enforcement investigation ends.

Notification will be provided directly to affected individuals by first-class mail, email, or telephone. The notice will be clear, concise, and written in plain language. To the extent available, it will include:

- A brief description of the breach or unauthorized release;
- The dates of the incident and the date of discovery, if known;
- The types of PII affected;
- An estimate of the number of records affected;
- A brief description of the Schools' investigation or plan to investigate;
- Protective steps and response actions, as applicable; and
- Contact information for representatives who can answer questions and provide assistance.

Contractors responsible for an incident must reimburse required notification costs under applicable law. Other applicable breach reporting duties remain in effect.

11. Publication, review, and implementation
Following adoption by the applicable governing board or boards, the Schools will publish this policy and the Parents' Bill of Rights on each School's website or school page, notify officers and employees, and maintain public contract-specific

supplements. The DPO will review the policy at least annually and recommend revisions when law, systems, or practices change.

The DPO will report annually to each applicable Board of Trustees on the number and disposition of reported breaches, if any, and a summary of complaints submitted under this policy. Material compliance concerns will be brought promptly to the applicable Board, together with proposed corrective actions or policy revisions.

The Schools will keep the DPO's contact information and linked resources current. Before publication, the Schools will enter the actual adoption and revision approval dates and replace all bracketed link placeholders with working public website links.