KIPP Capital Region
PUBLIC SCHOOLS

KIPP Capital Region Data Privacy and Security Policies

KIPP Capital Region Schools takes the confidentiality of information about our students and families seriously. Several federal and state laws and regulations protect the confidentiality of student educational records, including information that can be used to identify student-specific data, known as "personally identifiable information" or "PII."

These laws and regulations also place requirements on KIPP Capital and other parties to ensure that students' PII remains confidential and secure. New York State Education Department is making a stronger push to monitor the efficacy of school districts in meeting the mandates set forth by part 121 of Education Law 2-D. These actions are being taken by the state to ensure that student data privacy is being regarded with the utmost security, both in-district and by any approved third parties.

KIPP Capital Region's Data Privacy and Security Policies are intended to comply with the laws of the US Federal Government, the State of New York, and the NIST Cybersecurity Framework.

If you are a KIPP Capital student older than 18, the information shared below about an "eligible student" refers directly to you. This page also includes a notice to users of KIPP Capital's websites and applications.

Overview of Laws and Regulations

The federal laws that protect students' PII include:

- Family Educational Rights and Privacy Act (FERPA)
- Children's Online Privacy Protection Act (COPPA)
- Protection of Pupil Rights Amendment (PPRA)
- Individuals with Disabilities Education Act (IDEA)

State laws, such as N.Y. Education Law 2-d and the related regulations of the N.Y. State Commissioner of Education protect the confidentiality of student information.

Family Educational Rights and Privacy Act (FERPA)

FERPA is a federal law that protects the privacy of student educational records. FERPA gives families certain rights with respect to their student's education records.

If you are a student who is 18 years or older (also known as an eligible student), these rights belong to you, and not to your family or guardians.

In short, FERPA grants you the right to:

1. Inspect and review student's education records within 45 days after KIPP Capital receives your request and has verified your identity. Families and eligible students should submit a written

request to their school's principal. Your school will arrange for access and notify you of the time and place where you may inspect your requested records.
2. Request changes to student's education records when you believe they are inaccurate, misleading, or violate student privacy rights under FERPA.
3. Provide written consent before personally identifiable information (PII) in a student's education records is disclosed. Please note: in certain cases, FERPA allows disclosure without consent for directory information.
4. File a complaint with the U.S. Department of Education if you believe that KIPP Capital failed to comply with FERPA's requirements.
5. Receive notification of your rights under FERPA.

New York State Education Law § 2-d is a state law that places responsibilities on KIPP Capital and outside parties who receive student's PII from KIPP Capital through a written agreement. Education Law § 2-d requires KIPP Capital to do the following:

- Publish a Parents Bill of Rights for Data Privacy and Security. You can read more about the Parents Bill of Rights in the next section.
- Provide annual training to KIPP Capital staff who have access to student's PII.
- Ensure that the use and disclosure of PII benefits students.
- Ensure outside parties who receive student's PII have appropriate safeguards, policies, and practices in place to protect the data.
    - These safeguards must meet industry standards and best practices.
    - Examples of safeguards include encryption, firewalls, and password protection.
- Enter into written agreements with outside parties who receive student's PII from KIPP Capital. The written agreements outline how outside parties keep student's data confidential and secure.
- Notify families of unauthorized release of student data in a timely manner.

New York State Education Law § 2-d also requires outside parties that receive student information from KIPP Capital to address legal and privacy requirements in a written agreement with KIPP Capital. These safeguards promote transparency and provide additional protections for the benefit of our families. For example, outside parties must agree to the following:

1. Collect and disclose students' PII only as necessary and only for educational purposes.
2. Minimize the collection, processing, and transmission of PII.
3. Have safeguards in place to protect students' PII when it is stored or transferred. These safeguards must meet industry standards and best practices.
4. Not sell, use, or disclose PII for marketing, advertising, or other commercial purposes.
5. Train staff in applicable laws, policies, and safeguards associated with industry standards and best practices.

6. Not maintain copies of PII once it is no longer needed for the agreed upon educational purpose. Outside parties should permanently and securely delete PII no later than when the contract ends.
7. Abide by the Parent's Bill of Rights for Data Privacy and Security

The New York State Education Department has additional resources for you regarding the rights of student data regarding New York State Education Law § 2-d.

Parent's Bill of Rights for Data Privacy and Security

Under New York State Education Law § 2-d, if you are the parent or legal guardian of a student in KIPP Capital Region Public Schools, you have several rights regarding the privacy and security of student's PII, including the following:

- Student's personally identifiable information (PII) cannot be sold or released for any marketing or other commercial purposes.
- If student is under 18 years old:
    - You have the right to inspect and review the complete contents of a student's education records within 45 days of KIPP Capital receiving your request and verifying your identity.
    - You also have the right to request changes to student's education records when you believe they are inaccurate, misleading, or violate student's privacy.
    - Your rights extend to education records stored by KIPP Capital contractors or other outside parties on KIPP Capital 's behalf.
- You have the right to be notified if a breach or unauthorized release of a student's PII occurs.
- You have the right to make complaints about possible breaches and unauthorized disclosures of student's PII and to have such complaints addressed. KIPP Capital must provide you with a response no more than 60 calendar days from when we receive your complaint. If more time is needed, KIPP Capital will provide an explanation to you, along with an approximate date for a response.

When Consent is Not Required to Disclose Student PII

Generally, KIPP Capital must have written permission from a family or student who is 18 years or older to release any information from a student's education record. However, in certain cases, FERPA allows disclosure without consent. Cases permitting disclosure without consent include:

- Disclosure to KIPP Capital school officials who need to review education records to fulfill their professional responsibilities. These can include outside parties performing services or functions for KIPP Capital, such as contractors and consultants.
- When another school, district or education institution requests a student's education records to support enrollment or transfer.

- Circumstances in connection with financial aid applications that families or students filled out.
- Authorized government officials in connection with audits, evaluations, or certain other activities.
- Organizations conducting studies on behalf of KIPP Capital.
- Accrediting organizations carrying out accrediting functions.
- Families of students aged 18 and over who are considered dependents for Internal Revenue Service (IRS) tax purposes.
- Compliance with a judicial order or lawfully issued subpoena.
- Appropriate officials in connection with a health or safety emergency.
- Information that KIPP Capital has designated as "directory information," as outlined in more detail below.

Directory Information and Opt-Out Information

Certain types of basic information about families and students are considered "directory information." Schools can disclose directory information without your consent if, and only if, they first inform you of the following:

- The types of information they designate as "directory information"
- Who they are disclosing the directory information to and why they are disclosing it
- Your right to tell the school not to disclose the directory information (known as an "opt-out")
- The time frame you have to opt out of the disclosure

Schools may ask families to opt out of sharing some of their child's directory information, rather than ask all families to first consent to sharing the information, when they are celebrating students' achievements or noting their participation in activities with the school community. This may be particularly true for school-based publications and announcements of honors, awards or other recognition or participation in school activities, including:

- Graduation and honor rolls
- Receipt of scholarships or awards
- School publications that likely include student names and photographs, such as yearbooks, playbills, graduation lists, and participation in school sports and other activities

What is considered directory information?

Only a few pieces of information about students are eligible to be considered directory information. These include a student’s name, date of birth, school email address, user ID or other unique personal identifier used to communicate in electronic systems, participation in school activities, honors and

awards they've received, school enrollment and graduation details, their major field of study, their grade level and, in the context of their participation in school-based athletics, their height and weight.

There are also other types of student information that can be considered directory information, including home addresses, telephone numbers, and photographs; however, KIPP Capital considers these types of information to be sensitive in nature.

What is not considered directory information?

The following types of information are never treated as directory information: grades on assignments, courses, and exams; daily attendance statistics; race, ethnicity, or other demographic details; special education status; disciplinary history; and any other information that could be considered sensitive or a violation of privacy upon release. Social Security numbers also cannot be considered directory information.

Information About Data Security Incidents

Families and students who have reached age 18 have the right to be notified when their PII has been the subject of unauthorized acquisition, access, use, or disclosure.

How to Make a Complaint about Data Privacy Violations

Parents have the right to file complaints with KIPP Capital about possible privacy breaches of student data by the School's third-party contractors or their employees, officers, or assignees, or with NYSED. Complaints to the School may be submitted to the School's Data Protection Officer, and can be submitted online by clicking HERE or in writing to:

KIPP Capital Region Schools
C/O Data Protection Officer
321 Northern Blvd
Albany, NY 12201

Complaints to NYSED should be directed in writing to:
New York State Education Department
C/O Chief Privacy Officer
89 Washington Avenue, Albany NY 12234
Or emailed to: privacy@nysed.gov
Online form: https://www.nysed.gov/data-privacy-security/report-improper-disclosure

How to Request Changes to Education Records

You have the right to request changes to a student's education records, whether the records are held at a student's school, elsewhere within KIPP Capital, or by an outside party on behalf of KIPP Capital. This right

applies when you believe the record to be inaccurate, misleading, or otherwise in violation of a student's right to privacy. This right extends to education records, whether in physical or digital format, that are being maintained or stored by outside parties, including vendors KIPP Capital has contracted with or whose services they have purchased.

Please submit your request in writing (which includes email) to the student's school. The request must include the following:

- Student's name, date of birth, student identification number and school or program;
- Your name and your relationship to the child;
- A description of the information you believe to be inaccurate, misleading or in violation of student's right to privacy;
- If known, the outside entities to whom you believe KIPP Capital has disclosed the information; and
- The remedy or solution you are seeking.

If you wish to request changes to education records held by an outside party on behalf of KIPP Capital, please mail your request to:

KIPP Capital Region Schools
C/O Data Protection Officer
321 Northern Blvd
Albany, NY 12201

You will receive a response within 15 business days from when we receive your request. If your request is denied in whole or in part, you will be provided with notice of your right to appeal and to request a hearing.

Data Security and Privacy for Third-Party Contractors

Any Contractor that the School uses that may obtain PII will agree to the following terms which shall be incorporated into its contract for services ("the Contract") with the School and it shall adhere to the following provisions:

- The Contractor's storage use and transmission of student and teacher/principal PII shall be consistent with the School's Data Security and Privacy Policy available on the School's website.
- Contractor shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.
- The exclusive purposes for which the student data, teacher data or principal data will be used under the contract are set forth in Service Agreements, and such data will be used by the Contractor only for the term of the Contract.

- The Contractor shall maintain the following administrative, operational and technical safeguards and practices in place to protect PII, which shall align with the NIST Cybersecurity Framework, including:
- PII data will be protected using encryption while in motion and at rest by industry standard safeguards and best practices, such as firewalls, passwords, and two-factor authentication.
- PII will be stored in a manner as to protect its security and to mitigate any potential security risks. Specifically, all student data and/or teacher or principal data will be stored electronically. The security of this data will be ensured by industry standard safeguards and best practices, such as firewalls, passwords, and two-factor authentication.
- The Contractor shall ensure that no PII is disclosed to employees, subcontractors, or other persons or entities unless they have a legitimate educational interest and only for purposes necessary to provide services under the Contract.
- Contractor shall not disclose PII to any party other than those set forth in this Agreement, without prior written parental consent or unless required by law or court order. If disclosure of PII is required by law or court order, the Contractor shall notify the School no later than the time the PII is disclosed unless such notice is expressly prohibited by law or the court order.
- Contractor shall ensure that all employees, subcontractors, or other persons or entities who have access to PII 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). Contractor shall provide training to any employees, subcontractors, or other persons or entities to whom it discloses PII on the federal and state laws governing confidentiality of such data prior to allowing access.
- Absent some other state or federal mandate to retain data, upon expiration of the contract, the PII will be returned to the School and/or destroyed. Specifically, connections to source systems will be terminated immediately and all PII stored electronically on the Contractor side will be deleted within 90 days. All PII stored offline will be destroyed within 90 days.
- The Contractor shall take the following steps to identify breaches or unauthorized releases of PII and to notify the School upon learning of an unauthorized release of PII.
- Provide prompt notification to the School no later than seven (7) calendar days from date of discovery of a breach or unauthorized release of PII. Contractor shall provide notification to the School's data protection officer by phone and by email.
- Contractor shall cooperate with the School and law enforcement to protect the integrity of the investigation of any breach or unauthorized release of PII.
- Where a breach or unauthorized release is attributed to the Contractor, the Contractor shall pay for or promptly reimburse the School for the full cost of such notification. Contractor may also be subject to certain penalties, including but not limited to monetary fine, training on federal and state law regarding confidentiality of data, and preclusion from accessing PII from the School for up to five years.

- The Contractor acknowledges that it has received the Parents Bill of Rights and agrees to abide by its terms.
- The School shall publish this contract addendum on its website.

Notice to Users of KIPP Capital Web Sites and Applications

This notice informs you, as a user of our systems and applications, about how KIPP Capital Region Schools collect, use, and protect information about you through your use of this website. We also describe other policies that directly affect you, as users of these services. Please read this notice carefully before using our websites or applications. We may change this notice from time to time, and reserve the right to do so without advance notice. By accessing and using our websites and applications, you consent to these uses and any other uses.

Collection of Information

In order to improve the content and usability of Department websites and applications, we may automatically collect certain information from you, including:

- The Internet Protocol ("IP") address of your Internet Service Provider ("ISP") and/or computer.
- The Domain Name of your ISP and/or computer.
- The type and version of your operating system and browser (such as Internet Explorer, Opera, Firefox, Chrome, etc.).
- The date, time, and duration of your visit.
- Your clicks within the application.
- The web address of the previous site visited by your browser (if detectable).
  We also may request and collect information from you when you interact with our websites and applications, such as information you provide when creating an account, submitting an electronic form, participating in a survey, etc.

Use of Information and Privacy

We do not collect personally identifiable information for commercial or marketing purposes, and we do not sell the personally identifiable information we collect. The personally identifiable information we collect is stored in a secure environment.

We use and may share the information we collect to make sure our systems are up-to-date and compatible with other systems, and to improve services offered through applications and websites. We may also use it to fulfill our duties and for other educational purposes, including, but not limited to:

- Developing new application functionality;
- Providing notifications, alerts, or event updates;

- Responding to requests made under the Freedom of Information Law (FOIL), through subpoenas, court orders and other administrative, judicial and legal processes (however, we may withhold certain information if the law permits us to do so);
- Providing technical notices, updates, security alerts, and administrative messages;
- Responding to user comments, questions, and requests for customer service;
- Monitoring and analyzing trends, usage and activities in connection with services;
- Personalizing and improving services;
- Complying with any allowable educational purpose, applicable law, regulation, legal process, or governmental request; and
- Conducting statistical analyses for any of the above reasons.
  Certain laws and regulations govern our ability to share or otherwise disclose information about you that we collect. For example, as described in more detail above, disclosure and release of PII of our current and former students is governed by the Family Educational Rights and Privacy Act (FERPA). Other laws and regulations may apply, depending on the types of information involved.

We may monitor and review all content and traffic on Department-provided networks and applications. This includes traffic on or from devices that are owned by KIPP Capital, as well as devices not owned by the schools if KIPP Capital resources are being accessed or have been accessed from such devices.

Data Security

KIPP Capital takes reasonable measures to help protect its websites and applications and the information within them from loss, theft, misuse, unauthorized access, disclosure, alteration, and destruction.

If you receive or create a password when registering for any of our applications, you should not divulge this password to anyone. We will never ask for your password in a telephone call, fax, e-mail, or other form of unsolicited communication. When you are finished with an application, you should sign out of the application. If the browser you used to access the application is publicly accessible (such as on a computer at a public library or internet cafe), you should close the browser session and, if possible, clear any browser history, cookies, or other areas where your password might have been stored. Otherwise, you risk having information about you becoming available to third parties.

Cookies

Cookies are computer files that enable an application or website to distinguish between users. We use "temporary cookies" on some parts of our sites and applications, which expire when you close the browser session. We may also use "persistent cookies" to understand how people access and use our sites and applications.

KIPP Capital Region
PUBLIC SCHOOLS

You can customize most browsers to reject cookies, to accept or reject cookies after a visual warning, or to delete cookies. However, some application and website features may require cookies to function properly.