Privacy and security for student data and teacher and principal data

This Policy addresses Ascend's responsibility to adopt administrative, technical, and physical safeguards and controls to protect and maintain the confidentiality, integrity, and availability of its data, data systems, and information technology resources. Ascend is committed to maintaining the privacy and security of student data and teacher and principal data and will follow all applicable laws and regulations for the handling and storage of this data in the school and when disclosing or releasing it to others, including third-party contractors.

Student data refers to the personally identifiable information (PII) from the student records of an educational agency. Teacher or principal data means PII from the records of an educational agency that relate to the annual professional performance reviews of classroom teachers or principals.

Data collection transparency and restrictions

As part of its commitment to maintaining the privacy and security of student data and teacher and principal data, Ascend will take steps to minimize its collection, processing, and transmission of PII. Each school will monitor its data systems, develop incident response plans, limit access to PII to school employees, interns, volunteers, independent contractors, and third-party contractors who need such access to fulfill their professional responsibilities or contractual obligations, and destroy PII when it is no longer needed.

Additionally, Ascend will not sell PII 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.

Ascend will also 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 be maintained in accordance with law, regulation, and Ascend policy.

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

Chief Privacy Officer

Ascend will comply with its obligation to report breaches or unauthorized releases of student data or teacher or principal data to the Chief Privacy Officer, appointed by the Commissioner of Education.

Data Protection Officer

The Assistant Principal of Operations at each Ascend school will serve as the school's Data Protection Officer. The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures. The Data Protection Officer will serve as the main point of contact for the school's data privacy and security program. Ascend will ensure that the Data Protection Officer has the appropriate knowledge, training, and experience to administer these functions.

Data privacy and security standards

Ascend will use the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1) (the Framework) as the standard for its data privacy and security program.

Ascend will protect the confidentiality and privacy of student and teacher/principal PII while stored or transferred by:

a) Ensuring that every use and disclosure of PII by the school benefits students and the school by considering, among other criteria, whether the use and/or disclosure will:

   1. Improve academic achievement;

   2. Empower parents and students with information; and/or

   3. Advance efficient and effective school operations.

b) Not including PII in public reports or other public documents.

c) Using industry standard safeguards and best practices, such as encryption, firewalls, and passwords.

Ascend affords all protections under FERPA and the Individuals with Disabilities Education Act and their implementing regulations to parents or eligible students, where applicable.

Third-party contractors

School responsibilities

Ascend will ensure that whenever it enters into a contract or other written agreement with a third-party contractor who will receive student data or teacher or principal data from the school, the agreement will require that confidentiality of shared student data or teacher or principal data be maintained in accordance with federal and state laws and regulations, and Ascend policy. In addition, Ascend will ensure that the agreement includes a signed copy of the Parents' Bill of Rights for Data Privacy and Security and the third-party contractor's data privacy and security plan. The plan must, at a minimum:

a) Outline how the third-party contractor will implement all state, federal, and local data privacy and security contract requirements over the life of the contract, consistent with Ascend policy;

b) Specify the administrative, operational, and technical safeguards and practices the third-party contractor has in place to protect PII that it will receive under the contract;

c) Demonstrate that the third-party contractor complies with the requirements of 8 NYCRR Section 121.3(c);

d) Specify how officers or employees of the third-party contractor and its assignees who have access to student data or teacher or principal data receive training on the federal and state laws and regulations governing confidentiality of this data prior to receiving access;

e) Specify if the third-party contractor will utilize subcontractors and how it will manage those relationships and contracts to ensure PII is protected;

f) Specify how the third-party contractor will manage data privacy and security incidents that implicate PII, including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify Ascend; and

g) Describe whether, how, and when data will be returned to Ascend, transitioned to a successor contractor, at Ascend's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

Third-party contractor responsibilities

Each third-party contractor that enters into a contract or other written agreement with Ascend under which the contractor will receive student data or teacher or principal data from Ascend, is required to:

a) Adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework;

b) Comply with Ascend's data security and privacy policy, Education Law Section 2-d and its implementing regulations, and applicable laws impacting Ascend;

c) Limit internal access to PII to only those employees or subcontractors that need access to provide the contracted services;

d) Not use the PII for any purpose not explicitly authorized in its contract;

e) Not disclose any PII to any other party without the prior written consent of the parent or eligible student:

   1. Except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with law, regulation, and its contract with Ascend; or

   2. Unless required by law or court order and the third-party contractor provides notice of disclosure to NYSED, the Board, or the institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by law or court order;

f) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII in its custody;

g) Use encryption to protect PII in its custody while in motion or at rest; and

h) Not sell PII 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.

Where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal laws and contract with Ascend apply to the subcontractor.

If the third-party contractor has a breach or unauthorized release of PII, it will promptly notify Ascend in the most expedient way possible without unreasonable delay but no more than seven calendar days after the breach's discovery.

Click-wrap agreements

Periodically, Ascend staff may wish to use software, applications, or other technologies in which the user must "click" a button or box to agree to certain online terms of service prior to using the software, application, or other technology. These are known as "click-wrap agreements" and are considered legally binding contracts or other written agreements.

School staff are prohibited from using software, applications, or other technologies pursuant to a click-wrap agreement in which the third-party contractor receives student data or teacher or principal data from Ascend unless they have received prior approval from the school's Data Protection Officer or designee.

Ascend will develop and implement procedures requiring prior review and approval for staff use of any software, applications, or other technologies pursuant to click-wrap agreements.

Parents' bill of rights for data privacy and security

Ascend publishes its Parents' Bill of Rights for Data Privacy and Security (Bill of Rights) on its website. Additionally, Ascend will include the Bill of Rights with every contract or other written agreement it enters into with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from Ascend. The Bill of Rights will also include supplemental information for each contract the school enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the school.

Ascend's Bill of Rights can be found here.

Ascend will publish on its website the supplement to the Bill of Rights (i.e., the supplemental information described above) for any contract or other written agreement it has entered into with a third-party contractor that will receive PII from the School. The Bill of Rights and supplemental information may be redacted to the extent necessary to safeguard the privacy or security of Ascend's data and technology infrastructure.

Complaints of breach or unauthorized release of student data and/or teacher or principal data

Parents/guardians have the right to submit complaints about possible breaches of student data to the Chief Privacy Officer at NYSED. In addition, Ascend has established the following procedures for parents, guardians, eligible students, teachers, principals, and other school staff to file complaints with Ascend about breaches or unauthorized releases of student data and/or teacher or principal data:

a) All complaints must be submitted to the school's Data Protection Officer in writing, utilizing a complaint form available here.

b) Upon receipt of a complaint, the school will promptly acknowledge receipt of the complaint, commence an investigation, and take the necessary precautions to protect PII.

c) Following the investigation of a submitted complaint, the school will provide the individual who filed the complaint with its findings. This will be completed within a reasonable period of time, but no more than 60 calendar days from the receipt of the complaint by the school.

d) If the school requires additional time, or where the response may compromise security or impede a law enforcement investigation, the school will provide the individual who filed the complaint with a written explanation that includes the approximate date when the school anticipates that it will respond to the complaint.

Ascend 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.

Reporting a breach or unauthorized release

The Data Protection Officer will report every discovery or report of a breach or unauthorized release of student data or teacher or principal data within the school to the Chief Privacy Officer without unreasonable delay, but no more than ten calendar days after the discovery.

Each third-party contractor that receives student data or teacher or principal data pursuant to an agreement with Ascend will be required to promptly notify the school of any breach resulting in an unauthorized release of the data by the contractor or its assignees. This notification will happen without unreasonable delay, but no more than seven calendar days after the discovery of the breach. In the event of notification from a third-party contractor, the school will in turn notify the Chief Privacy Officer of the breach or unauthorized release of student data or teacher or principal data no more than ten calendar days after it receives the contractor's notification.

The Chief Privacy Officer is required to investigate reports of breaches or unauthorized releases of student data or teacher or principal data by third-party contractors. Upon the belief that a breach or unauthorized release constitutes criminal conduct, the Chief Privacy Officer is required to report the breach and unauthorized release to law enforcement.

Notification of a breach or unauthorized release

The school will notify affected parents, eligible students, teachers, and/or principals in the most expedient way possible but no more than 60 calendar days after the discovery of a breach or unauthorized release of PII by the school or the receipt of a notification of a breach or unauthorized release of PII from a third-party contractor, unless that notification would interfere with an ongoing investigation by law enforcement or cause further disclosure of PII by disclosing an unfixed security vulnerability. Where notification is delayed under these circumstances, the school will notify parents, eligible students, teachers, and/or principals within seven calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends. Notification will be directly provided to the affected parent, guardian, eligible student, teacher, or principal by first-class mail to their last known address, by email, or by telephone.

The Data Protection Officer must annually report to the Board of Education on data privacy and security activities and progress, any changes to data privacy and security measures, the number and disposition of reported breaches, if any, and a summary of any complaints submitted pursuant to Education Law 2-d.

Annual data privacy and security training

Ascend will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations. All officers and staff who have access to PII must complete this training annually.

Adoption Date
September 30, 2020