iKeepProfile
National Student Clearinghouse StudentTracker for High Schools

Introduction

The iKeepSafe California Privacy Program is available to operators and service providers of websites and online services, data management systems and other technologies that are, in whole or in part, intended for use in and by schools, and which may collect, store, process or otherwise handle student data.

This *iKeepProfile* is intended to assist you in determining whether the National Student Clearinghouse StudentTracker® for High Schools service complies with FERPA, SOPIPA, California AB 1584, and other California state laws and district policies. It indicates that StudentTracker for High Schools has been assessed for alignment with the iKeepSafe California Privacy Program Guidelines.

The *iKeepProfile* is not legal guidance, nor does it guarantee or otherwise assure compliance with any federal or state laws. If you have questions on how to use the *iKeepProfile* to support your school's compliance efforts, please contact your school attorney.[1]

Product Overview

National Student Clearinghouse StudentTracker for High Schools:

http://www.studentclearinghouse.org/high_schools/studenttracker/

StudentTracker® for High Schools is a unique service designed to help high schools and districts more accurately gauge the college success of their graduates by answering such key questions as: How many of my high school graduates enroll in college? Do they persist and graduate from college? How long does it take for them to get their degree? Do they go in or out of state? Do they attend a 2- or 4-year school? Which colleges do they most commonly attend? Did any students go on to college who started 9th grade in my high school, but did not graduate?

Agreement

As a participant in the iKeepSafe California Privacy Program, the National Student Clearinghouse agrees:

A. Family Educational Rights and Privacy Act ("FERPA") (20 U.S.C. Section 1232g)

1. It will act as a School Official as defined by FERPA. As such, it is under the direct control of the applicable school with regard to use and maintenance of education records.

2. Education records continue to be the property of and under the control of the school district; and the National Student Clearinghouse is willing to stipulate as such in a contract or terms of use with the school district.

3. It will use education records only for the purposes authorized by the school, and will not disclose personally identifiable information from education records to other parties unless it has received specific authorization from the school to do so and it is otherwise permitted by FERPA.

4. It will provide a means by which a parent, legal guardian, or eligible student may review personally identifiable information in the student's records and correct erroneous information. Each school using the StudentTracker for High Schools service has its own user account that allows access to its data in its respective SFTP logical partition. An authorized school employee can access its data at any time. Should a school need assistance from the National Student Clearinghouse to access its data, it can contact its designated account representative for support.

5. It will take actions to help ensure the security and confidentiality of education records. The National Student Clearinghouse maintains a comprehensive Information Security Program based on ISO 27000 controls to ensure implementation and oversight of management, technical and operational controls.

6. It will conduct annual training related to data privacy and information security responsibilities, including FERPA requirements, for all employees and contractors. Additional training is also required for those with significant IT roles and aspects of student data management.

7. It is willing to include contract provisions or other terms of use detailing rights related to transfer of students' personally identifiable information from education records to the school or its designated third party upon request by the school or upon expiration or termination of the agreement, and subsequent deletion of students' personally identifiable information held by the National Student Clearinghouse and third parties operating in connection with the National Student Clearinghouse.

8. It will not make material changes to its privacy and security policies, including adding practices around new or additional data collection, or changes that may lessen the previously noted protections without prior notice to the school, separate from any notice in a "click wrap" agreement.

B. California AB 1584 (Buchanan) Privacy of Pupil Records: 3rd-Party Digital Storage & Education Software (Education Code section 49073.1)

1. Pupil records obtained by the National Student Clearinghouse from the LEA continue to be the property of and under the control of the LEA. The School retains full ownership rights to the information in the education records it provides to the National Student Clearinghouse.

2. The National Student Clearinghouse does not collect or store any pupil-generated content.

3. The National Student Clearinghouse shall not use any information in a pupil record for any purpose other than those required or specifically permitted by the StudentTracker for High Schools Agreement.

4. Parents, legal guardians, or eligible pupils can review personally identifiable information in the pupil's records and correct erroneous information by contacting the educational institution that provided the data in question to the National Student Clearinghouse.

5. The National Student Clearinghouse is committed to maintaining the security and confidentiality of pupil records. To that end, the National Student Clearinghouse has taken the following actions: (a) limiting employee access to student data based on roles and responsibilities; (b) conducting background checks on employees who have access to student data; (c) requiring that a new employee or contractor receive privacy training, including FERPA, as a condition of employment or engagement; (d) providing employees and contractors with security and privacy policies in writing; and (e) protecting personal information with physical, electronic and procedural safeguards that are appropriate to the sensitivity of the information, in order to protect it from unauthorized access, release or use.

6. In the event of an unauthorized disclosure of a pupil's records, the National Student Clearinghouse will promptly notify the educational institution unless specifically directed not to make such notification by law enforcement. The notification will include the nature of the incident, the information compromised and the action taken. The National Student Clearinghouse will keep the educational institution fully informed until the incident is resolved.

7. The National Student Clearinghouse will delete personally identifiable data upon request of the LEA and/or upon expiration of the services agreement.

8. The National Student Clearinghouse agrees to work with the LEA to ensure compliance with FERPA and the Parties will ensure compliance by providing parents, legal guardians or eligible students access to, or correction of, student data. The Clearinghouse agrees to facilitate access and correction of data shared under this Agreement by referring the parents, legal guardians or eligible students to the educational institution that provided the data in question to the Clearinghouse.

9. The National Student Clearinghouse prohibits users from using personally identifiable information in pupil records in order to engage in targeted advertising.

C. SB 1177 - Student Online Personal Information Protection Act ("SOPIPA")

Prohibitions:

1. The National Student Clearinghouse does not engage in targeted advertising on its website or any other website using information acquired from students or student records.

2. The National Student Clearinghouse StudentTracker for High Schools service does not use information, including persistent unique identifiers, created or gathered by the site, service, or application, to amass a profile about a K–12 student, except in furtherance of K–12 school purposes.

3. The National Student Clearinghouse does not and will not sell or rent students' personal information, nor does its StudentTracker for High Schools service provide students' personal information to any third party, except as described in this Profile.

4. The National Student Clearinghouse's StudentTracker for High Schools service does not disclose student information obtained under the service, unless for legal, regulatory, judicial, safety or operational improvement reasons.

Obligations:

1. The National Student Clearinghouse is committed to maintaining the security and confidentiality of student records as noted herein.

2. The National Student Clearinghouse will delete district-controlled student information when requested by school district.

3. The National Student Clearinghouse will disclose student information when required by law, for legitimate research purposes, and for school purposes to educational agencies.

Security Protocols

The National Student Clearinghouse has a comprehensive Information Security Program in place that ensures the confidentiality, integrity and availability of systems, networks and data. The following is a general overview of their data security protocols:

Data in Transit
All uploads are transferred to the SFTP server via TLS or SSH using FIPS 140-2 validated AES-256 cryptography to the respective school or customer's logical disk partition. Once on the SFTP server, data is stored using 256 bit Advanced Encryption Standard (AES). File integrity checking by SHA256 and SHA512 file verification uses built-in file verification mechanisms to guarantee delivery and validate that transferred files have not been compromised in any way and ensure that the source and destination are exact matches.

Data at Rest
Data is encrypted using 256 bit Advanced Encryption Standard (AES), a FIPS 140-2 validate cryptographic module.

Data Storage
Data is stored on servers and the Storage Area Network (SAN) in the data center located at the Clearinghouse's headquarters. The SAN utilizes a Redundant Array of Independent Disks (RAID) configuration, encrypted using AES 256-bit cryptography. Backup tapes are stored with Iron Mountain and are also encrypted using AES 256-bit.

Data Center Security
National Student Clearinghouse employees are issued photo identification badges for monitoring and providing access to the Clearinghouse's premises. Non-employees, such as consultants, working at the Clearinghouse are issued a temporary security badge. Photo identification or security badges are required for access to all office space occupied by the Clearinghouse. The Computer Room is located within a locked suite; access to this area is limited to authorized staff as is access to storage areas containing confidential information. Visitors are escorted by staff while on the premises. Access to the building during non-business hours requires an authorized photo identification badge. All building entrances and exits are monitored with video surveillance equipment and require a key card. Unauthorized access to any National Student Clearinghouse suite triggers an alarm. A security company monitors the doors and has been provided with telephone notification procedures.

System Security Certification
National Student Clearinghouse has been certified by a Qualified Security Assessor (QSA) in the Payment Card Industry Data Security Standards (PCI-DSS), which are the unified base requirements for all credit card association data security programs. Association data security programs, such as Visa CISP, MasterCard SDP, American Express and Discover Card, all require PCI-DSS. The Clearinghouse uses a certified vendor, TrustWave, for its PCI-DSS compliance program. TrustWave Site Certification fulfills all requirements of PCI-DSS, Visa CISP, MasterCard SDP, American Express DSS, and Discover Card programs.

System Security Accreditation & Assurance
In addition to its ongoing PCI DSS certification process, National Student Clearinghouse contracts annually with third-party security firms to perform security assessments, including external and internal network penetration testing. National Student Clearinghouse staff members responsible for managing systems subscribe to Department of Homeland Security (DHS) United States Computer Emergency Response Team (U.S. CERT) advisories, System Administration, Networking and Security (SANS) Institute advisories, and other relevant sources providing current information about security vulnerabilities. In addition, the Clearinghouse also employs staff with current information security certifications, such as the Certified Information Systems Security Professional (CISSP) to ensure that it stays current with industry best practices.

Access

Access to data on National Student Clearinghouse systems is protected by a layered defense of physical (operational) and technical controls such as firewalls, authentication systems and role based access models on systems and network platforms. This approach complements the management controls put in place by the National Student Clearinghouse policies, procedures, standards and guidelines. The security concept of "least-privilege" is implemented to ensure users are only granted access to data that is necessary to perform the duties of their position. Access is granted by written authorization and controlled by policy.

Security Awareness, Training & Educational

Training in information security is provided to all employees upon hire and then annually; additional information is provided on a regular basis. Consultants receive the same training regarding FERPA and data privacy and security that employees of the Clearinghouse receive, and are subject to the same access controls. The National Student Clearinghouse's written operating policies and procedures include technical, physical and operational safeguards. All staff (i.e., employee, contractor, consultant, temporary, volunteer, intern, etc.) must comply with the Clearinghouse's

Access to Audit

Once per year, the National Student Clearinghouse will provide schools utilizing its StudentTracker for High Schools service with:

☐ audit rights to the school's data

☑ access to the results of the National Student Clearinghouse's or its third-party security audit

Product Data List

Student Data Required		General Purpose of Data Collection
1	First and last name	Data is matched with PSED records to provide school with information on its students postsecondary education; de-identified data is aggregated into national reports to allow high schools to benchmark their results
2	Date of birth	Data is matched with PSED records to provide school with information on its students postsecondary education; de-identified data is aggregated into national reports to allow high schools to benchmark their results
3	FERPA Block	Collected for possible future services
4	Diploma Type	Indicator that students are diploma recipients
5	Graduation Date	Provides the beginning date for the postsecondary search
6	School ACT code	Used to identify the school in the Clearinghouse system

Optional Student Data Fields		General Purpose of Data Collection
1	Social Security Number	Used by some schools as an identifier and is returned to school with postsecondary data.
2	ID Number	Used by some schools as an identifier and is returned to school with postsecondary data.
3	Gender	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field.
4	Ethnicity	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field.
5	Economically Disadvantaged Indicator	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field.
6	8th Grade Math Assessment Tier	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field.
7	8th Grade ELA/Reading Assessment Tier	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field.

8	English Learning Indicator	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field.
9	Number of Math Semesters Completed	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field.
10	Dual Enrollment Indicator	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field.
11	Disability	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field.
12	Program Code	Allows the Clearinghouse to provide the school/district with additional levels of postsecondary outcomes based on this field in detail reporting.
13	Middle Name	Used for matching purposes.
14	Name Suffix	Used for matching purposes.
15	Previous Last Name	Used for matching purposes.
16	Previous First Name	Use for matching purposes.
17	State High School Assessment Tier–Reading	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field.
18	State High School Assessment Tier - Math	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field.

Third Parties

The National Student Clearinghouse does not sell, lease, provide or otherwise share individual information with any unauthorized third parties. There are no third parties service providers operating within the StudentTracker for High Schools service.

The National Student Clearinghouse may contract with third party consultants and other contractors to perform business functions or services on their behalf. The National Student Clearinghouse has agreements in place with all third party consultants and contractors with access to student personal information to ensure they only use the information for purposes necessary to deliver the authorized service and to ensure they maintain the confidentiality and security of the information. Third party consultants and other contractors shall not use any information in a pupil record for any purpose other than those required or specifically permitted by the StudentTracker for High Schools Agreement.

Accuracy Statement

The National Student Clearinghouse hereby confirms the accuracy and truthfulness of all information contained in the profile, and has authorized iKeepSafe to make the profile available to any interested schools.

Signed and agreed:

DocuSigned by:
Mary Chapin
1149528EC22C49B...
(Signature)

Mary Chapin
Chief Legal Officer
National Student Clearinghouse

06/29/17

The National Student Clearinghouse StudentTracker for High Schools has been reviewed and found in alignment with iKeepSafe's FERPA and California Privacy Program Guidelines as indicated by this product profile. The National Student Clearinghouse StudentTracker for High Schools has been awarded the iKeepSafe FERPA and California Privacy Program badges.

DocuSigned by:
Holly Hawkins
B0E6FFA00A18442...
(Signature)

Holly Hawkins
President & CEO
iKeepSafe

06/29/17

Copyright

Disclaimer

[1] By using the California Privacy Assessment Program or accepting any materials related to the California Assessment Program, you expressly acknowledge and agree that neither Internet Keep Safe Coalition, their affiliates, subsidiaries, or designees nor each of their respective officers, directors, employees or agents (collectively, Associates), can guarantee, certify or ensure that you are in compliance with FERPA, SOPIPA, California AB 1584, or any other state or federal laws. You understand that the California Privacy Program does not constitute legal or any other type of professional advice and the California Privacy Seal is not a legal determination.

You further acknowledge that the California Privacy Assessment Program is not officially recognized by the U.S. Department of Education or any other legislative or regulatory body, and the program does not provide any legal safe harbor. You are encouraged to consult with your attorney. Under no circumstances shall the Internet Keep Safe Coalition, or their Associates be liable for any direct, indirect, incidental, special or consequential damages that result from you not being in compliance with FERPA, SOPIPA, California AB 1584, or for any claim that you are not in compliance with these and other applicable laws. You acknowledge and represent that it is your sole responsibility to evaluate whether or not you are in compliance with these and other laws.