iKeepSafe

iKeepProfile
National Student Clearinghouse
StudentTracker for High Schools

Introduction

The iKeepSafe 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 National Student Clearinghouse: Student Tracker for High Schools complies with FERPA and SOPIPA. It indicates that National Student Clearinghouse has been assessed for alignment with the iKeepSafe FERPA and SOPIPA Privacy Program Guidelines.

Product Overview

National Student Clearinghouse: StudentTracker for High Schools

StudentTracker for High Schools is a unit-record postsecondary outcome reporting Data-as-a-Service/Software-as-a-Service platform. Authorized education organizations may submit high school graduate cohorts for matching and outcome reporting. StudentTracker for High Schools reports on student outcomes longitudinally for up to 8-years post high school graduation.

Agreement

As related to the Family Educational Rights and Privacy Act ("FERPA") (20 U.S.C. Section 1232g), National Student Clearinghouse agrees, with respect to its StudentTracker for High Schools service:

1. Student records obtained by National Student Clearinghouse from an educational institution continue to be the property of and under the control of the educational institution. The educational institution retains full ownership rights to the personal information and education records it provides to the National Student Clearinghouse.
2. National Student Clearinghouse will not use any information in a student record (i) for any purpose other than those specifically permitted in contracts with institutions; or (ii) in a manner inconsistent with the National Student Clearinghouse Terms and Conditions and Privacy Policy.
3. Parents, legal guardians, or eligible students may request to review personally identifiable information in the student's records and correct erroneous information by contacting their educational institution.
4. National Student Clearinghouse is committed to maintaining the security and confidentiality of student records. Towards this end, we take the following actions:
    a. we limit employee access to student data to only those employees with a need to such access to fulfill their job responsibilities;
    b. we conduct background checks on our employees that may have access to student data;
    c. we conduct regular employee privacy and data security training and education; and
    d. we protect personal information with technical, contractual, administrative, and physical security safeguards in order to protect against unauthorized access, release or use.
5. In the event of an unauthorized disclosure of a student's records, National Student Clearinghouse will promptly notify administrators unless specifically directed not to provide such notification by law enforcement officials.
6. Upon written request, National Student Clearinghouse will delete or de-identify personal information when it is no longer needed, with any deletion or de-identification to be completed according to the terms of our agreement with the educational institution, or at the direction or request of the educational institution.
7. National Student Clearinghouse agrees to work with educational institutions to ensure compliance with FERPA and the Parties will ensure compliance by providing parents, legal guardians or eligible students with the ability to inspect and review student records and to correct any inaccuracies therein as described above.
8. National Student Clearinghouse prohibits using personally identifiable information in student records to engage in targeted advertising.
9. National Student Clearinghouse will not make material changes to our Terms of Use or Privacy Policy, reducing protections, including making significant changes impacting the collection, use, disclosure or retention of data collected without prior notice to the educational user.

As related to the Student Online Personal Information Protection Act (SB 1177 -"SOPIPA"), National Student Clearinghouse agrees, with respect to its StudentTracker for High Schools service:

1. National Student Clearinghouse does not conduct targeted advertising via the National Student Clearinghouse service or on any other website using information about a K-12 student, their families/guardians or educators acquired from a use of the technology.

2. National Student Clearinghouse does not use information, including persistent unique identifiers, created or gathered by the National Student Clearinghouse service to amass a profile about a K–12 student, their families/guardians or educators except in furtherance of K–12 school purposes.

3. National Student Clearinghouse does not and will not sell, rent, or otherwise provide personally identifiable information to any third party for monetary gain.

4. National Student Clearinghouse does not disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

Data Review Process

The National Student Clearinghouse provides administrators direct access to the personally identifiable information that they provide to the National Student Clearinghouse via product functionality. Administrators can also contact the National Student Clearinghouse for access to all personal information on file by contacting National Student Clearinghouse directly by the following methods:

General inquiries related to privacy may be directed to: privacy@studentclearinghouse.org.

You may also contact us at 2300 Dulles Station Blvd., Suite 220, Herndon, VA 20171 or at (703) 742-4200.

Security Protocols

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 via SFTP using FIPS 140-2 validated 256-bit AES encryption to secure files during transfers using TLS connections. File integrity checking uses built-in file verification mechanisms to guarantee delivery and validate that transferred files have not been compromised in any way and to ensure that the source and destination are exact matches.

Data at Rest

Data is encrypted using 256 bit AES, a FIPS 140-2 validated cryptographic module. The storage area network (SAN) used for storage is equipped with disks that encrypt the data while it is at rest within that device. The SAN utilizes a Redundant Array of Independent Disks (RAID) configuration, and the application encrypts PII data at the database level using AES 256 encryption.

Data Storage

Stored data is maintained at the Clearinghouse's DR site in Middletown VA. The Clearinghouse maintains the connection using a dedicated and encrypted point to point connection. The data is encrypted using FIPS-140-2 approved 256 AES encryption.

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 an exhaustive security assessment, 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; additional information is provided on a regular basis. 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 information security policies; those who do not are subject to disciplinary action up to and including termination.

Personnel

Background Checks: All employees with access to student data have undergone criminal background checks.

Training: Employees of National Student Clearinghouse will receive annual privacy and security training that includes FERPA.

Access: Access to student data is role-based; limited to those employees who need access to perform job responsibilities.

Employees are given access to the minimum services that are required for their job function.

Access to Audit

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

Once per year, National Student Clearinghouse will provide schools with:

[X] audit rights to the school's data

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

Data Breach

In the event of an unauthorized disclosure of a student's records, National Student Clearinghouse will promptly notify administrators, unless specifically directed not to provide such notification by law enforcement officials. Notification shall identify:

a. the date and nature of the unauthorized use or disclosure;
b. the PII used or disclosed;
c. general description of what occurred including who made the unauthorized use or received the unauthorized disclosure;
d. what National Student Clearinghouse has done or shall do to mitigate any effect of the unauthorized use or disclosure;
e. what corrective action National Student Clearinghouse has taken or shall take to prevent future similar unauthorized use or disclosure; and
f. who at National Student Clearinghouse the administrator can contact. National Student Clearinghouse will keep the user fully informed until the incident is resolved.

National Student Clearinghouse will notify impacted administrators (s) within 72 hours upon the confirmation of a breach of security that results in the unauthorized release, disclosure or acquisition of student information.

Data Deletion

National Student Clearinghouse states they will retain participating institution's information for as long as the account is active, or as needed to provide our services. Participating institutions may contact us at the email address at contracts@studentclearinghouse.org should they wish to cancel their account or request that we no longer use the information to provide services. We will retain and use participating institution's information as necessary to comply with our legal obligations, resolve disputes, and enforce our agreements.

Participating Institutions that send the Clearinghouse student data in order to receive Clearinghouse services may request the correction or deletion of such data by contacting their Clearinghouse contact, by sending an email to StudentTracker@studentclearinghouse.org.

Research

National Student Clearinghouse:

Research Center: Through aggregated longitudinal data outcomes reporting, the Research Center facilitates better educational policy decisions leading to improved student outcomes. The Clearinghouse periodically produces several aggregate reports on student enrollment, movement, and other important student outcomes. Learn more at: https://nscresearchcenter.org/.

FERPA Guidelines for Studies exception: An education record may be disclosed to an organization conducting a study for or on behalf of an educational institution, in order to develop, validate, or administer predictive tests; administer student aid programs; or improve instruction.

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' post-secondary 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' post-secondary education; de identified data is aggregated into national reports to allow high schools to benchmark their results
4	FERPA Block	Indicator is used to ensure secondary student record is not used in future Clearinghouse services or products.
5	Diploma Type	Indicator allows users and the Clearinghouse to aggregate and disaggregate outcomes by diploma type earned.
6	Graduation Date	Provides the beginning date for the post-secondary search
7	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 post-secondary data.
2	ID Number	Used by some schools as an identifier and is returned to school with post-secondary data
6	Gender	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field
7	Ethnicity	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field
8	Economically Disadvantaged Indicator	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field
9	8th Grade Math Assessment	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field
10	8th Grade ELA/Reading Assessment	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field
11	English Learning Indicator	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field
12	Number of Math Semesters Completed	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field
13	Dual Enrollment Indicator	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field

14	Disability	Allows the Clearinghouse to provide the school/district with additional levels of aggregate postsecondary outcomes based on this field
15	Program Code	Allow user to add additional classifications to data submissions for aggregation/disaggregation by the user later.

Third Parties

National Student Clearinghouse does not sell, trade, lease or loan the personal information they collect or maintain, in the course of providing the service, to any third party for any reason, including direct marketers, advertisers, or data brokers.

National Student Clearinghouse contracts with other third-party companies to perform business functions or services on their behalf and may share PII with such third parties as required to perform their functions. National Student Clearinghouse has agreements in place with all third parties 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. The agreements align with National Student Clearinghouse' data privacy and security policies and expectations.

National Student Clearinghouse utilizes the following third-party vendors:

Google Analytics: End user behavior within the application for the purpose of improving the service

Accuracy Statement

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:

(Signature)

Mary Chapin

Mary C. Chapin, Chief Legal Officer, Vice President & Corporate Secretary
National Student Clearinghouse
2300 Dulles Station Blvd., Suite 220, Herndon, VA 20171
703.742.3261 http://www.studentclearinghouse.org

11/6/19

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. National Student Clearinghouse StudentTracker for High Schools has been awarded the iKeepSafe FERPA and California Privacy Program badges.

DocuSigned by:
Amber Lindsay
4936610B3823488...
(Signature)

Amber Lindsay
President & CEO
iKeepSafe

10/21/19

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.