Castle Software, Inc.
Parents Bill of Rights - Supplemental Information Addendum for Ed Law 2-d

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY*

The privacy and security of personally identifiable student data is of paramount importance. A student's personally identifiable information cannot be sold or released for any commercial purposes. State and federal laws protect the confidentiality of students' personally identifiable information, and safeguards associated with industry standards and best practices, such as encryption, firewalls, and password protection, must be in place when such data is stored or transferred.

Consistent with the adoption by the New York State Legislature of the Common Core Implementation Reform Act of 2014, all parents have the following rights:

- To inspect and review the complete contents of their child's education record, as defined in the District's Student Records policy;

- To access a complete list of all student data elements collected by the State, which is available for public review at http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx , or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234;

- To have complaints about possible breaches of student data heard and determined. Complaints should be directed in writing to the local education agency or Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234, or by email to the Chief Privacy Officer at CPO@mail.nysed.gov.

*In the event the Commissioner of Education issues an enhanced Bill of Rights and/or promulgates regulations setting forth additional elements to be included in the Parents' Bill of Rights, Castle Software, Inc. reserves the right to revise this document accordingly.

Supplemental Information Addendum

In the course of complying with its obligations under the law and providing educational services to school and district residents, the local education agency or district ("Subscriber") has entered into an agreement with a third-party contractor Castle Software, Inc. ("Castle"). Pursuant to this agreement, Castle may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the Subscriber enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the Subscriber, the following supplemental information will be included with this Bill of Rights:

1) The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;

The Castle Learning application, provided by Castle Software, Inc. ("Castle"), holds minimal student/teacher enrollment data to establish login credentials and class rosters within Castle Learning, which is used for online assignments and assessments for academic progress in core and supplemental academic subjects.

2) How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, 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);

All Castle employees and content contractors, regardless of whether they access student or teacher data to provide the service or not, receive annual FERPA training and are required to review and acknowledge compliance with the Written Information Security Plan Policy (WISPP), which is provided with this addendum and which outlines the Castle compliance methodology. Many Subscribers purchase Method Test Prep and/or GradeCam through Castle. Castle reviews their compliance measures as well, but they are individually responsible for their own EdLaw 2-d compliance. Castle is a reseller for both. We use secure API's to exchange basic user identification information for single signon.

3) The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the Subscriber, and/or whether, when, and how the data will be destroyed);

The duration of the contract ("Term") is subject to the length of the subscription established on the accepted proposal/quote to the Subscriber and/or as confirmed by the Subscriber's purchase order. Upon expiration of the Term, unless renewed by the Subsciber for a subsequent Term, the Subscriber's data will be destroyed approximately ninety to one hundred twenty (90 to 120) days following the expiration date of the term. This time period for data destruction is used as often school districts realize the need to renew a lapsed subscription following the start of a school year. Delaying the destruction date enables the re-activation of the Subscriber's user accounts without losing valuable prior history (i.e. teachers are able to re-use prior assingments and assessments they have created). When a final data destruction date is reached, the data is destroyed by

first deleting/purging it from the Castle Learning database and then the data is subsequently removed from nightly backups once the backup retention period is reached. The local retention period is two weeks and the offsite backup retention period is ninety (90) days. As Castle only holds minimal enrollment data for logins, class rosters, assignments and assessments, it is uncommon for Subscribers to request copies of this data upon termination; however, if desired, the data may be extracted and provided to the Subscriber in csv or other requested format via a secure file download on a time and materials basis.

4) If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;

Parent [student, eligible student, teacher or principal] may challenge the accuracy of data by submitting their concerns to the Subsciber or the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to CPO@mail.nysed.gov. If concerns are submitted directly to Castle, Castle will forward the concern to the established Castle Subscriber administrative contact in order to coordinate resolving the concern.

5) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated;

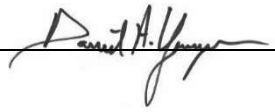
The Castle Learning software is hosted from a dedicated to Castle environment within a highly secure SOCII compliant Rackspace data center. Rackspace manages the physical computing, networking environment and local backup system, but Rackspace employees do not access the application or the database/data that runs on top of the physical environment. Only Castle technical operations resources, who need to access the servers in order to provide the Castle Learning application service, do so remotely via secure VPN connections. Application support staff provide support services by logging in to the application as end-users do.

and

6) Address how the data will be protected using encryption while in motion and at rest.

The Castle Learning application is encrypted in motion via https (secure certificate/SSL/TLS 1.2 or higher) and sensitive data elements are encrypted at the column level in our database at rest. All backups are encrypted at rest as well. In addition to the local networking/firewall protection that is managed by Rackspace, Castle Learning is further protected from external threats by a web application firewall.

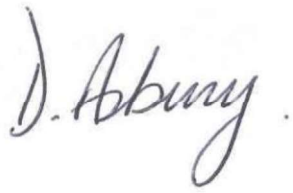
We agree to abide by the Subscriber's Parents' Bill of Rights for Data Privacy and Security.

Name: Daniel A. Youngren Date: 4/18/2020 Signature: 

Company: Harris Education Solutions/Castle Software, Inc. Product (If different): Castle Learning

HARRIS SCHOOL SOLUTIONS
WRITTEN INFORMATION SECURITY PROGRAM POLICY ("WISPP")

Corporate Officer: Dennis Asbury, Senior Executive Vice President



Signature: _____

REVISION

Rev	Date	Author	Type	Description	Approval
1.0	06/08/17	Katie Rose	Major	Revised original WISP to reflect FERPA requirements and new Harris Corporate Policies.	Tim Fitzgerald
1.1	02/15/2018	Tim Fitzgerald	Minor	Revised DSC & BUR section, miscellaneous document revisions.	Tim Fitzgerald
1.2	11/1/2019	Katie Rose	Minor	Annual Review	Dennis Asbury

OBJECTIVE:

The objective of Harris School Solutions ("HSS") in the development and implementation of this comprehensive Written Information Security Program Policy ("WISPP"), is to create effective administrative, technical and physical safeguards for the protection of Education Records as defined in 34 CRF §99.3 ("Education Records"), and the Personally Identifiable Information contained therein as defined in 34 CFR §99.3 ("PII") and the confidential records of our customers' end users, including but not limited to our customers' employees (i.e. teachers and principals) and students, (cumulatively, all 'end users'), and to comply with our obligations under the Family Educational Rights and Privacy Act ("FERPA") at 20 USC 1232g and any applicable state laws or regulations (the "regulations").

The WISPP sets forth our procedure for evaluating and addressing our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting Education Records and PII of all end users.

PURPOSE:

The purpose of the WISPP is to better: (a) ensure the security and confidentiality of Education Records and PII, (b) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and (c) protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft, fraud, misuse or invasion of privacy.

SCOPE:

In formulating and implementing the WISPP, Harris School Solutions ("HSS") has addressed and incorporated the following protocols:

(a) identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Education Records or PII;

(b) assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Education Records and PII;

(c) evaluated the sufficiency of existing policies, procedures, information systems, and other safeguards in place to control risks;

(d) designed and implemented a WISPP that puts safeguards in place to minimize those risks; and

(e) implemented regular monitoring of the effectiveness of those safeguards.

DATA SECURITY COORDINATOR & BUSINESS UNIT REPRESENATATIVE:

Harris School Solutions has designated a Data Security Coordinator to implement, supervise and maintain the WISPP. The Data Security Coordinator ("DSC") may be an individual and / or may also be comprised of one or more members of the Corporate IT ("CIT") staff and shall work with a designated Business Unit Representative ("BUR") to carry out the following data security responsibilities, and as assigned below.

(a) Implementation of the WISPP including all provisions outlined in the Operational Protocol set forth below.

Responsibility: DSC & BUR

(b) Training of all employees.

Responsibility: BUR (in conjunction with their Human Resources Advisor and oversight by the Governance, Risk and Compliance Committee (GRCC))

(c) Regular testing of the WISPP's safeguards that are pertinent to the Business Unit level;

Responsibility: DSC & BUR

(d) Evaluating the ability of any of our third party service providers to implement and maintain appropriate security measures for the Education Records or PII to which HSS has permitted said third party to access, and requiring such third party service providers by contract to implement and maintain appropriate security measures.

Responsibility: BUR

(e) Reviewing the scope of the security measures in the WISPP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing Education Records or PII.

Responsibility: BUR (providing evidence to DSC as appropriate)

(f) Conducting an annual training session for all HSS officers, managers, employees and independent contractors, including any temporary and contract employees who have access to Education Records or PII on the elements of the WISPP and notifying the GRCC of the completion of such training.

Responsibility:

- DSC in conjunction with the GRCC to identify changes to existing requirements.
- BUR to deliver training (via a Human Resources Advisor)

(g) Tracking of assets assigned to HSS employees in accordance with the Corporate Asset Tracking Policy.

Responsibility: DSC & CIT

INTERNAL RISK MITIGATION POLICIES:

To guard against internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Education Records or PII, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

(a) HSS will only collect personal information of clients, customers, customer's employees or students (i.e. end-users) where it is necessary to accomplish our legitimate business transactions or to comply with any and all regulations. See HSS' Privacy Policy and Harris' Corporate Policy for Responsible Use of IT Resources.

(b) Access to records containing Education Records or PII shall be limited to those employees whose duties, relevant to their job description, have a legitimate need to access said records, and only for this legitimate job-related purpose. See Harris' Corporate Information Access Management Policy.

(c) Written and electronic records containing Education Records or PII shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements. HSS' business records needs and associated retention and secure destruction periods are set at three (3) years. See Harris' Corporate Back-Up, Device and Media Controls Policy.

(d) Transmission of Education Records and PII must be kept to a minimum necessary and protected with appropriate safeguards. See Harris' Corporate Transmission Security Policy and Corporate Email Policy.

(e) A copy of the WISPP is to be distributed to each current Harris HSS employee and to each new employee within 30 days of the date of their employment. Employees should advise their manager or the Data Security Coordinator of any activities or operations which appear to pose risks to the security of Education Records or PII. See Harris' Corporate Information Access Management Policy and Corporate Data Incident Handling Policy.

(f) An internal HSS training session for all current HSS employees will be held annually to detail the provisions of the WISPP, and as otherwise detailed in this policy. See Harris' Corporate Security Awareness and Training Policy.

(g) Terminated employees must return all records containing Education Records or PII, in any form, in their possession at the time of termination. This includes all data

stored on any portable device and any device owned directly by the terminated employee. See Harris' Corporate Information Access Management Policy and the Corporate Back-Up, Device and Media Controls Policy.

(h) A terminated employee's physical and electronic access to records containing Education Records or PII shall be disabled at the time of termination. This shall include remote electronic access to personal records, voicemail, internet, and email access. All keys, keycards, access devices, badges, company IDs, business cards, and the like shall be surrendered at the time of termination. See Harris' Corporate Information Access Management Policy.

(i) Disciplinary action will be applicable to violations of the WISPP, irrespective of whether personal data was actually accessed or used without authorization.

(j) All security measures including the WISPP shall be reviewed annually to ensure that the policies contained in the WISPP are adequate to meet all applicable regulations.

(k) Should HSS' business practices change in a way that impacts the collection, storage, and/or transportation of records containing Education Records or PII the WISPP will be reviewed to ensure that the policies contained in the WISPP are adequate to meet all applicable regulations.

(l) The Data Security Coordinator or his/her designee(s) shall be responsible for all review and modifications of the WISPP and shall fully consult and apprise management of all reviews including any recommendations that improves security arising from the review.

(m) Access to Education Records and PII is restricted to approved active user accounts and in accordance with Harris' Corporate Information Access Management Policy.

(n) Current employees' user ID's and passwords shall conform to accepted security standards. All passwords shall be changed at least every 90 days, or more often as needed. See Harris' Corporate Access Control Policy, Corporate Password Policy and Corporate Policy for Responsible Use of IT Resources.

(o) Employees are required to report suspicious or unauthorized use of Education Records or PII to a supervisor, the Data Security Coordinator or his/her designee(s). See Harris' Corporate Data Incident Policy.

(p) Whenever there is an incident that requires notification pursuant to any applicable regulations the Data Security Coordinator or his/her designee(s) shall host a mandatory post-incident review of events and actions taken, if any, in order to determine how to alter security practices to better safeguard Education Records and PII. See Harris' Corporate Data Incident Policy.

EXTERNAL RISK MITIGATION POLICIES:

All system security software including malicious code protection, internet security including firewall protection, operating system security patches, and applicable software products shall be reasonably up-to-date and installed on any HSS computer that stores or processes Education Records or PII. (Refer to Harris' Corporate Policy for Responsible Use of IT Resources, Corporate Network Management Policy and Corporate Protection from Malicious Software Policy.)

There shall be secure user authentication protocols in place that:

(a) Control user ID and other identifiers;

(b) Assigns passwords in a manner that conforms to accepted security standards, or applies use of unique identifier technologies;

(c) Control passwords to ensure that password information is secure.

See Harris' Corporate Access Control Policy, Corporate Password Policy and Corporate Policy for Responsible Use of IT Resources.

Education Records and PII shall not be removed from the business premises in electronic or written form absent legitimate business need and use of reasonable security measures, as described in this policy. See Harris' Corporate Policy for Responsible Use of IT Resources.

OPERATIONAL PROTOCOL:

The Operational Protocol shall be reviewed and modified as deemed necessary at a meeting of the Data Security Coordinator, the corresponding BU Representative and any other personnel responsible for the security of Education Records and PII. The review meeting shall take place during the first quarter of each year. Any modifications to the Operational Protocol shall be published in an updated version of the WISPP. At the time of publication, a copy of the WISPP shall be distributed to all current HSS employees and to new hires on their date of employment.

1. Recordkeeping Protocol:

HSS will only collect personal information of clients and customers and employees that is necessary to accomplish HSS' legitimate business transactions or to comply with any and all regulations. (See HSS' Privacy Policy and Harris' Corporate Information Access Management Policy.)

Within 90 days of the publication of the WISPP or any update, the Data Security Coordinator or his/her designee(s) shall perform an audit of all relevant HSS records to determine which records contain Education Records or PII, assign those files to the appropriate secured

storage location, and to redact, expunge or otherwise eliminate all unnecessary Education Records or PII in a manner consistent with the WISPP.

Any Education Records or PII stored shall be disposed of when no longer needed for business purposes or required by law for storage. Disposal methods must be consistent with those prescribed by the WISPP.

Any paper files containing Education Records or PII of clients, employees, students or end-users shall be stored in a locked filing cabinet or room at the end of each day.

All employees are prohibited from keeping unsecured paper files containing Education Records or PII in their work area when they are not present (e.g. lunch breaks).

Paper or electronically stored records containing Education Records or PII shall be disposed of in a manner that complies with any applicable regulations, which may include the following (which services may be provided by a third party specializing in such procedures):

(a) paper documents containing Education Records or PII shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;

(b) electronic media and other non-paper media containing Education Records or PII shall be destroyed or erased so that the Education Record or PII cannot practicably be read or reconstructed.

Electronic records containing Education Records or PII shall not be stored or transported on any portable electronic device, sent or transmitted electronically to any portable device, or sent or transported electronically to any computer, portable or not, without being encrypted. The only exception shall be where there is no reasonable risk of unauthorized access to the Education Record or PII or it is technologically not feasible to encrypt the data as and where transmitted. (Also refer to Harris' Corporate Transmission Security Policy, Corporate Remote Access Policy and Corporate Email Policy.)

If necessary for the functioning of individual Business Units, the Business Unit Executive Vice President, in consultation with the Data Security Coordinator or his/her designee(s), may develop specific rules for that Business Unit that ensure reasonable restrictions upon access and handling of files containing Education Records or PII and must comply with all WISPP standards. Business Unit rules are to be published as an addendum to the WISPP. (Refer to Harris' Corporate Portable Computing Devices Policy.)

2. Access Control Protocol:

All HSS computers shall restrict user access to those employees having an authorized and unique log-in ID. (Refer to Harris' Corporate Access Control Policy, Facility Access Controls Policy and Corporate Password Policy.)

All visitors who are expected to access areas other than common space or are granted access to office space containing Education Records or PII shall be required to sign-in and/or accompanied by an authorized employee.

All visitors are restricted from areas where files containing Education Records or PII are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files containing Education Records or PII are stored. (Refer to Harris' Corporate Facility Access Controls Policy.)

All systems with an internet connection or any HSS computing device that stores or processes Education Records or PII must have a reasonably up-to-date version of malicious code protection software installed and active at all times.

3. Third Party Service Provider Protocol:

Any HSS service provider or individual that receives, stores, maintains, processes, or otherwise is permitted access to any file containing Education Records or PII ("Third Party Service Provider") shall be required to meet the following standards (where such Third Party Service Providers will include third parties who provide off-site backup storage copies of all HSS electronic data; paper record copying or storage service providers; contractors or vendors working with HSS' customers and having authorized access to HSS records):

(a) Any contract with a Third Party Service Provider who will have access to the Education Records or PII of end-users shall require the Service Provider to implement security standards consistent with the security protocols defined in this WISPP.

(b) It shall be the responsibility of HSS to obtain reasonable confirmation that any Third Party Service Provider is capable of meeting security standards consistent with this WISPP. (See HSS' Privacy Policy.)

BREACH OF DATA SECURITY PROTOCOL:

Should any employee know of a security breach at any of HSS' facilities, or that any unencrypted Education Record or PII has been lost, stolen or accessed without authorization, or that encrypted Education Records or PII along with the access code or security key has been acquired by an unauthorized person or for an unauthorized purpose ("Security Incident"), the following protocol is to be followed.

(a) Employees are to notify the Data Security Coordinator, the Director of CIT, Legal Counsel, Privacy Officer, Business Unit Representative or the employee's manager in the event of a known or suspected Security Incident. The Data Security Coordinator, Director of CIT, Legal Counsel or Privacy Officer, Business Unit Representative or the employee's manager must then report any such known or suspected Security Incident to their Executive Vice President who shall also ensure that the Data Security Coordinator, Privacy Officer and Legal Counsel are aware of the Security Incident.

(b) The Data Security Coordinator or his/her designee(s) shall be responsible for drafting a security breach notification to be provided to the relevant persons, as appropriate. The security breach notification shall include the following:

(1) A detailed description of the nature and circumstances of the Security Incident;
(2) The number of applicable persons affected at the time the notification is submitted;
(3) The steps already taken relative to the incident;
(4) Any steps intended to be taken relative to the incident subsequent to the filing of the notification; and
(5) Information regarding whether law enforcement officials are engaged in investigating the incident.

(Also see Harris' Corporate Data Incident Policy and Harris Security Incident Response Plan)