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 sign on.

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 afinal 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 removedfrom 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 requestedformat 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;

Castle is hosted in the Amazon Web Services (AWS) us-east-1 region (Virginia), which complies with and is audited for, numerous regulatory standards. All data is stored in the United States.

Access to Castle data is tightly controlled on a need-to-know basis and all users are subject to the regulations and continued education dictated by the Harris Information Security Program. Databases and SQL servers containing sensitive PII are accessible only by authorized administrators and developers using a secure VPN connection.

We utilize multiple layers of firewall to tightly control ingress/egress traffic, in addition to leveraging CloudFlare's industry-leading Enterprise WAF (Web Application Firewall) to sanitize web requests and mitigate DDoS attacks.

CrowdStrike Falcon Complete XDR is utilized across all servers and endpoints for Anti-Virus, Malware, Ransomware and AI-driven Anomaly prevention and detection. HES also utilizes CrowdStrike's 24/7 SOCaaS (Security-Operations-Center-as-a-service) offering which provides all the security functions performed by a traditional, in-house SOC, including network monitoring, log management, threat detection and intelligence, incident investigation and response, reporting, and risk and compliance.

CIS V8 controls provide the basis for our security framework. The Rapid7 product suite provides automated scanning for routine hardening recommendations for Cloud architecture, applications, and server configuration.

Castle is committed to complying with all relevant regulatory standards and will

regularly review and update its data management practices ensuring compliance with changing requirements.

and

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

All data in Castle is encrypted in motion and at rest within AWS using an industry standard AES-256 encryption algorithm to ensure data confidentiality and integrity. The Castle Learning application is encrypted in motion via https (SSL/TLS 1.2 or higher) and sensitive data elements are encrypted at the column level within the database. All backups are encrypted at rest and are purged after 90 days.

Paper or electronically stored records containing Education Records, Teacher or Principal Data, or End User Confidential Information will be disposed of in a manner that complies with the Corporate Back-Up, Device and Media Controls Policy. All purged PII is securely deleted by AWS to ensure that it cannot be recovered, reconstructed, or accessed by unauthorized parties.

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

Name: Diva Mayeau Date: 07/01/2024 Signature: 

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

Liberty Source LLC
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.

In accordance with New York Education Law § 2-d, the Subscriber (i.e. school/district) wishes to inform the community of the following:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.

2. Parents have the right to inspect and review the complete contents of their child's education record.

3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by the State is available for public review at https://www.nysed.gov/data-privacy-security/student-data-inventory, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website https://www.nysed.gov/data-privacy-security/report-improper-disclosure.

**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, Liberty Source LLC 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 Liberty Source LLC ("Liberty Source"). Pursuant to this agreement, Liberty Source 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;

ELABORATION ON PURPOSE

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 Liberty Source 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 Liberty Source compliance methodology.

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);

ELABORATION ON CONTRACT LENGTH AND DATA DISPOSAL

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 Subscriber 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 Liberty Source, Liberty Source will forward the concern to the established Liberty Source 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;

- **Tango Software is hosted in the Amazon Web Services (AWS) us-east-1 region (Virginia), which complies with and is audited for, numerous regulatory standards. All data is stored in the United States.**
- **Access to Tango Software data is tightly controlled on a need-to-know basis and all users are subject to the regulations and continued education dictated by the Harris Information Security Program. Databases and SQL servers containing sensitive PII are accessible only by authorized administrators and developers using a secure VPN connection.**
- **Multiple layers of firewall are utilized to tightly control ingress/egress traffic, in addition to leveraging CloudFlare's industry-leading Enterprise WAF (Web Application Firewall) to sanitize web requests and mitigate DDoS attacks.**
- **CrowdStrike Falcon Complete XDR is utilized across all servers and endpoints for Anti-Virus, Malware, Ransomware and AI-driven Anomaly prevention and detection. Liberty Source also utilizes CrowdStrike's 24/7 SOCaaS (Security-Operations-Center-as-a-service) offering which provides all the security functions performed by a traditional, in-house SOC, including network monitoring, log management, threat detection and intelligence, incident investigation and response, reporting, and risk and compliance.**
- **CIS V8 controls provide the basis for our security framework. The Rapid7 product suite provides automated scanning for routine hardening recommendations for Cloud architecture, applications, and server configuration.**
- **Liberty Source is committed to complying with all relevant regulatory standards and will regularly review and update its data management practices ensuring compliance with changing requirements.**

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

- **All data in Tango Software is encrypted in motion and at rest within AWS using an industry-standard AES-256 encryption algorithm to ensure data confidentiality and integrity. The Tango Software application is encrypted in motion via https (SSL/TLS 1.2 or higher) and sensitive data elements are encrypted at the column level within the database. All backups are encrypted at rest and are purged after 90 days.**
- **Paper or electronically stored records containing Education Records, Teacher or Principal Data, or End User Confidential Information will be disposed of in a manner that complies with the Corporate Back-Up, Device and Media Controls Policy. All purged PII is securely deleted by AWS to ensure that it cannot be recovered, reconstructed, or accessed by unauthorized parties.**

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

Name: Diva Mayeau **Date**: 06/20/25

Signature: 

Company: Harris Education Solutions / Liberty Source LLC

eDoctrina Corporation
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.

In accordance with New York Education Law § 2-d, the Subscriber (i.e. school/district) wishes to inform the community of the following:

A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at http://www.nysed.gov/data-privacy-security/student-data-inventory, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website http://www.nysed.gov/data-privacy-security/report-improper-disclosure.*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, EDoctrina 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 eDoctrina Corporation ("eDoctrina"). Pursuant to this agreement, eDoctrina 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 exclusive purpose for which eDoctrina is being provided access to Protected Data is to provide Subscriber with the functionality of the Product(s) listed below. eDoctrina agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the Agreement. Protected Data received by eDoctrina, or any of eDoctrina's subcontactors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

- eDoctrina Educator Suite (Curriculum Bundle: Unit Planning, Lesson Planning, Power Standards, Curriculum Presenter/Recorder, Scope and Sequence Reports, Curriculum Mapping; Assessment Bundle: Assessment Building, Online Assessments, Paper Assessments, Performance-Based Assessments, Copier Scanning, Web Camera Scanning, Data Reporting; RTI/MTSS Bundle: Student Goals, Student Forms)
- eDoctrina Accountability Suite (OBS*e*RVE Module, SLO/SGO Tool, Educator Effectiveness/Performance Pay, Staff Forms & Improvement Plans)
- Add-Ons (PD30, R*e*PORT Cards, B*e*HAVE, SOLe)
- Question Banks (Examgen, Certica Solutions Navigate Item Bank, Inspect Question and Assessment Bank)

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 eDoctrina 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 eDoctrina compliance methodology.

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 eDoctrina 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. 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 eDoctrina, eDoctrina will forward the concern to the established eDoctrina 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;

eDoctrina is hosted in the Amazon Web Services (AWS) us-east-1 region (Virginia), which complies with and is audited for, numerous regulatory standards. All data is stored in the United States.
Access to eDoctrina data is tightly controlled on a need-to-know basis and all users are subject to the regulations and continued education dictated by the Harris Information Security Program. Databases and SQL servers containing sensitive PII are accessible only by authorized administrators and developers using a secure VPN connection.
We utilize multiple layers of firewall to tightly control ingress/egress traffic, in addition to leveraging CloudFlare's industry-leading Enterprise WAF (Web Application Firewall) to sanitize web requests and mitigate DDoS attacks.
CrowdStrike Falcon Complete XDR is utilized across all servers and endpoints for

Anti-Virus, Malware, Ransomware and AI-driven Anomaly prevention and detection. HES also utilizes CrowdStrike's 24/7 SOCaaS (Security-Operations-Center-as-a-service) offering which provides all the security functions performed by a traditional, in-house SOC, including network monitoring, log management, threat detection and intelligence, incident investigation and response, reporting, and risk and compliance.
CIS V8 controls provide the basis for our security framework. The Rapid7 product suite provides automated scanning for routine hardening recommendations for Cloud architecture, applications, and server configuration.
eDoctrina is committed to complying with all relevant regulatory standards and will regularly review and update its data management practices ensuring compliance with changing requirements.

and

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

All data in eDoctrina is encrypted in motion and at rest within AWS using an industry standard AES-256 encryption algorithm to ensure data confidentiality and integrity. The eDoctrina application is encrypted in motion via https (SSL/TLS 1.2 or higher) and sensitive data elements are encrypted at the column level within the database. All backups are encrypted at rest and are purged after 90 days.
Paper or electronically stored records containing Education Records, Teacher or Principal Data, or End User Confidential Information will be disposed of in a manner that complies with the Corporate Back-Up, Device and Media Controls Policy. All purged PII is securely deleted by AWS to ensure that it cannot be recovered, reconstructed, or accessed by unauthorized parties.

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

Name: Diva Mayeau Date: 1/1/2025

Signature: 

Company: Harris Education Solutions/eDoctrina Corporation

Product (If different): eDoctrina Educator and Accountability Suites and Add-ons