EZSCHOOLPAY PARTICIPATION AGREEMENT

THIS EZSCHOOLPAY PARTICIPATION AGREEMENT (this "Agreement") is entered into this _first_____ day of _____August_____, 2017____ (the "Effective Date") by and between N. Harris Computer Corporation ("Harris") and _Elbert School District #200_____ ("Customer").

In consideration of the mutual promises contained herein and for other goods and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

1. Definitions. As used in this Agreement, the following terms have the following meaning:
   (a) "N. Harris Computer Corporation" is the operator of the Payment Service and the licensor of the SPOS.
   (b) "Business Day" means any day in which Harris is open for the regular conduct of its business, and specifically excluding Harris holidays.
   (c) "License Agreement" means the Harris End User License Agreement between Harris and Customer for Customer's use and the support and maintenance of the SPOS.
   (d) "Notice" means any notice or communication between the parties required or allowed hereunder and made in accordance with the requirements of Section 8(d). (e) "Payment Service" means the service offered by Harris to Users that allows Users to make on-line payments to Harris for credit to Student's meal accounts with Customer, currently known as the EZSchoolPay.com payment service.
   (f) "Customer" means the school, school district, or other organization who is a party to this Agreement and who is a licensee of the SPOS and the provider of meals and meal services to Students.
   (g) "SPOS" means the Meal Tracker® or eTrition® Site Point of Sale software used by and licensed to Customer under the License Agreement.
   (h) "Student" means a person enrolled at Customer and to whose benefit a User has utilized the Payment Services.
   (i) "Term" means that period defined in Section 7(a).
   (j) "User" means the parent or guardian of a Student or other person legally authorized to use and who has entered into an agreement with Harris for the Payment Service for the benefit of a Student.

2. Online Credits & Other Payments. Upon receipt by Harris of a User payment request conforming to Harris' criteria, Harris shall initiate a credit entry in the amount of the payment from such User (Harris less any convenience fee and/or other charges assessed by the Customer) to the account of the Student in the SPOS. Customer agrees to accept such credit in the full amount for immediate access and use by the Student in accordance with Customer's agreement with the Student and/or the Student's parent, guardian, or other authorized person concerning the purchase of meals and/or other Customer payments. Customer agrees that it will not discriminate against credits and payments from or through Harris and will honor such payments on the same basis as any other payments or form of payments received by Customer for the purchase of meals and/or other Customer payments.

3. Customer Obligations. In addition to such other obligations of the Customer as outlined herein during the Term, Customer shall:

IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.

(d) Harris shall use its reasonably commercial efforts to process User credits and payments in a timely manner in accordance with the terms and conditions of this Agreement. OTHER THAN FOR FOREGOING SENTENCE, NEITHER HARRIS, ITS DESIGNEES, EMPLOYEES, AGENTS, OR AFFILIATES WILL BE LIABLE FOR CLAIMS, LOSSES, ACTIONS, DAMAGES, OR INJURY RESULTING FROM ANY FAILURE OF PERFORMANCE, ERROR, OMISSION, INACCURACY, INTERRUPTION, DEFECT, UNTIMELINESS OR UNAUTHENTICITY OF ANY INFORMATION, DELAY OR INTERRUPTION IN OPERATION OR TRANSMISSION, INTERCEPTION OF TRAFFIC SENT OR RECEIVED, COMMUNICATION LINE FAILURE, SECURITY BREACH, EAVESDROPPING, THEFT OR DESTRUCTION OR UNAUTHORIZED ACCESS TO, ALTERATION OF, OR USE OFINFORMATION, OR THE USE OF THE FACILITIES.

(e) IN NO EVENT WILL HARRIS, ITS DESIGNEES, EMPLOYEES, AGENTS, OR AFFILIATES BE LIABLE FOR ANY PUNITIVE DAMAGES, OR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR SIMILAR DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT. IN ALL CASES HARRIS' MAXIMUM LIABILITY SHALL NOT EXCEED THE LESSER OF CUSTOMER'S ACTUAL, DIRECT DAMAGES RESULTING FROM HARRIS' BREACH OR HARRIS' NET PROFITS RELATED TO THE BREACH.

6. Term and Termination.

(a) This Agreement shall begin on the Effective Date and unless earlier terminated as provided herein, shall continue for a period of one (1) year after the Effective Date. Unless terminated hereunder, this Agreement shall automatically renew for successive periods of one (1) year each.

(b) Either party may terminate this Agreement: (i) at any time, with or without cause, by giving the other party sixty (60) days prior written Notice of such termination; (ii) immediately and without Notice in the event of bankruptcy, insolvency, liquidation, winding up, reorganization, protection or relief of the other party (whether voluntary of involuntary) under any law of any jurisdiction, or upon issuance of any order for relief or the appointment of a receiver, trustee, or other similar official for the other party; and (iii) ten (10) Business Days after Notice by a party of a breach of this Agreement by the other party and such other party has not cured such breach within such 10-day period.

(c) Harris, at its option, may immediately terminate this Agreement upon termination or expiration of the License Agreement.

(d) The termination or expiration of this Agreement shall not impact and this Agreement shall still apply to any transaction between Harris and a User entered into prior to the effective date of the termination or expiration and for a reasonable period thereafter as necessary for Harris to make the credits and payments applicable thereto and for Customer to honor such credits as outlined herein. The provisions of Sections 4, 5, 6, and 7 shall survive the termination or expiration of this Agreement.

7. Generally.

(a) Independent Parties. The parties acknowledge each is independent of the other, and Harris may engage in other business activities at its sole discretion. This Agreement does not in any way create or constitute a relationship of agency, employment, partnership, or a joint venture between the parties.

(b) Non-Assignment. Customer's rights and obligations under this Agreement may not be assigned without the prior written consent of Harris. This Agreement shall benefit the parties and their respective successors and permitted assigns.

(c) Force Majeure. Customer agrees that Harris shall not be liable for any losses and damage, including consequential damages, detention, or delay or failure to perform resulting from causes beyond the control of Harris including, but not limited to, acts of God, acts or omissions on the part of Customer, delays in transportation or communications, failure to obtain supplies and services not caused by the negligence of Harris, changes in governmental regulations, war, or civil disturbance.

(d) Notices. All Notices shall be in writing and delivered personally, or by certified mail, email, postage prepaid, addressed to the parties at the addresses set forth on the signature page below, or such other address as a party shall provide by notice. Notices shall be deemed received three (3) days after mailing when the above procedures are followed or when actually received.

Confidentiality and Non-Disclosure Addendum

_____, Inc. ("Vendor") and Elbert School District No. 200 (the "District"), agree that this Addendum shall supplement and supersede the _____ AGREEMENT dated _____, 2017 (including without limitation the provisions, if any, related to end-user licensing and student data privacy)

Definition of "Data": Data include all Personally Identifiable Information (PII) and other non-public information. Data include, but are not limited to, student data, metadata, and user content. All PII will be treated in accordance with the Colorado Student Transparency and Security Act, the Family Education Rights and Privacy Act (FERPA), and all applicable state and federal law.

Rights and License to Data: All rights, including all intellectual property rights, in the Data shall remain the exclusive property of the District, and Vendor has a limited, nonexclusive license solely for the purpose of performing its obligations and services. The Vendor does not have any rights, implied or otherwise, to Data, content, or intellectual property, except as expressly needed to perform its services. This includes the right to sell or trade Data. Any Data held by Vendor will be made available to the District upon request by the District.

Data Use and Collection: Vendor will only collect and use Data necessary to fulfill its duties, provide services, and improve services to the District. Vendor is prohibited from mining Data for any purposes other than those agreed to by the parties. Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is prohibited. Data and/or programs stored on District equipment will not be duplicated and/or stored by the Vendor on other media without the District's express permission. The District understands that Vendor may rely on one or more subcontractors to perform services. The Vendor agrees to share the names of these subcontractors with District upon request. All subcontractors and successor entities of Vendor will be subject to the terms of this Addendum.

Data Transfer or Destruction: Vendor will ensure that all Data in its possession and in the possession of any subcontractors, or agents to which the Vendor may have transferred Data, are destroyed or transferred to the District under the direction of the District when the Data are no longer needed for their specified purpose, at the request of the District.

Security Controls: Vendor will store and process Data in accordance with industry standard practices. This includes appropriate administrative, physical, and technical safeguards to secure Data from unauthorized access, disclosure, and use. Vendor will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. Vendor will also have a written incident response plan, to include prompt notification of the District in the event of a security or privacy incident, as well as industry standard practices for responding to a breach of PII.

Modification of Terms of Service: Vendor agrees to notify District should any of the conditions change with the Vendor's Privacy Policy. Changes to Vendor's practices, Privacy Policy, or End User License Agreement that conflict with existing statutes may result in immediate termination of any vendor contract with the district. The District may terminate any Vendor contract with the District in the event the Vendor fails to cure a material breach of this Addendum within thirty (30) days of receiving written notice from the District.

Vendor Signature	Title	Date
District Signature	Title	Date
	Superintendent	8/1/17

Confidentiality and Non-Disclosure Addendum

N. Harris Computer Corporation ("Vendor") and Elbert School District No. 200 (the "District"), agree that this Addendum shall supplement and supersede the AGREEMENT dated July 25, 2017 (including without limitation the provisions, if any, related to end-user licensing and student data privacy)

Definition of "Data": Data include all Personally Identifiable Information (PII) and other non-public information. Data include, but are not limited to, student data, metadata, and user content. All PII will be treated in accordance with the Colorado Student Transparency and Security Act, the Family Education Rights and Privacy Act (FERPA), and all applicable state and federal law.

Rights and License to Data: All rights, including all intellectual property rights, in the Data shall remain the exclusive property of the District, and Vendor has a limited, nonexclusive license solely for the purpose of performing its obligations and services. The Vendor does not have any rights, implied or otherwise, to Data, content, or intellectual property, except as expressly needed to perform its services. This includes the right to sell or trade Data. Any Data held by Vendor will be made available to the District upon request by the District.

Data Use and Collection: Vendor will only collect and use Data necessary to fulfill its duties, provide services, and improve services to the District. Vendor is prohibited from mining Data for any purposes other than those agreed to by the parties. Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is prohibited. Data and/or programs stored on District equipment will not be duplicated and/or stored by the Vendor on other media without the District's express permission. The District understands that Vendor may rely on one or more subcontractors to perform services. The Vendor agrees to share the names of these subcontractors with District upon request. All subcontractors and successor entities of Vendor will be subject to the terms of this Addendum.

Data Transfer or Destruction: Vendor will ensure that all Data in its possession and in the possession of any subcontractors, or agents to which the Vendor may have transferred Data, are destroyed or transferred to the District under the direction of the District when the Data are no longer needed for their specified purpose, at the request of the District.

Security Controls: Vendor will store and process Data in accordance with industry standard practices. This includes appropriate administrative, physical, and technical safeguards to secure Data from unauthorized access, disclosure, and use. Vendor will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. Vendor will also have a written incident response plan, to include prompt notification of the District in the event of a security or privacy incident, as well as industry standard practices for responding to a breach of PII.

Modification of Terms of Service: Vendor agrees to notify District should any of the conditions change with the Vendor's Privacy Policy. Changes to Vendor's practices, Privacy Policy, or End User License Agreement that conflict with existing statutes may result in immediate termination of any vendor contract with the district. The District may terminate any Vendor contract with the District in the event the Vendor fails to cure a material breach of this Addendum within thirty (30) days of receiving written notice from the District.

Vendor Signature	VP of Sales Title	7/25/2017 Date
District Signature	Superintendent Title	7/25/17 Date

Harris School Solutions
Written Information Security Plan (WISP)

Table of Contents

I. OBJECTIVE:

The objective of Harris School Solutions (HSS) in the development and implementation of this comprehensive written information security program ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of personal information (personally identifiable information "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 any applicable laws or regulations (the "regulations").

The WISP sets forth our procedure for evaluating and addressing our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of all end users.

For purposes of this WISP, the term "Student Data" means personally identifiable information from student records that Third Party Contractor receives from a School District. The term "Teacher or Principal Data" shall mean personally identifiable information from the records of a School District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release. "Personally Identifiable Information" ("PII") as applied to Student Data, means personally identifiable information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA), at 20 USC 1232g.

II. PURPOSE:

The purpose of the WISP is to better: (a) ensure the security and confidentiality of Student Data, Teacher or Principal data and other personal information, (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.

III. SCOPE:

In formulating and implementing the WISP, Harris School Solutions 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 personal information;

(b) assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;

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

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

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

IV. DATA SECURITY COORDINATOR:

Harris School Solutions has designated a Data Security Coordinator to implement, supervise and maintain the WISP. The Data Security Coordinator may be an individual and / or may also be comprised of one or more members of the Corporate IT staff and shall be responsible for the following:

(a) Implementation of the WISP including all provisions outlined in Section VII of this policy: Daily Operational Protocol;

(b) Training of all employees;

(c) Regular testing of the WISP's safeguards;

(d) Evaluating the ability of any of our third party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access, and requiring such third party service providers by contract to implement and maintain appropriate security measures;

(e) Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information; and

(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 personal information on the elements of the WISP.

V. INTERNAL RISK MITIGATION POLICIES:

To guard against internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, 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.

(b) Access to records containing personal information 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.

(c) Written and electronic records containing personal information shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements. HSS' frequent business records needs and associated retention and secure destruction periods are set at three (3) years.

(d) A copy of the WISP is to be distributed to each current Harris HSS employee and to each new employee on the beginning date of their employment. Employees are encouraged and invited to advise their manager or the Data Security Coordinator of any activities or operations which appear to pose risks to the security of personal information.

(e) Internal HSS training session for all current HSS employees will be held during the first-half of 2016 to detail the provisions of the WISP, and as otherwise as detailed in this policy.

(f) Terminated employees must return all records containing personal data, 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.

(g) A terminated employee's physical and electronic access to records containing personal information shall be restricted 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.

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

(i) All security measures including the WISP shall be reviewed annually in the first quarter of each such year to ensure that the policies contained in the WISP are adequate to meet all applicable regulations.

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

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

(l) If applicable, the Data Security Coordinator or his/her designee(s) shall maintain a secured and confidential master list of all lock combinations, passwords, and keys. The list will identify which employees possess keys, keycards, or other access devices and that only approved employee have been provided access credentials.

(m)The Data Security Coordinator or his/her designee(s) shall ensure that access to personal information in restricted to approved and active user accounts.

(n) Current employees' user ID's and passwords shall conform to accepted security standards. All passwords shall be changed at least annually, or more often as needed (e.g. seasonally).

(o) Employees are required to report suspicious or unauthorized use of personal information to a supervisor, the Data Security Coordinator or his/her designee(s).

(p) Whenever there is an incident that requires notification pursuant to any 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 personal information.

VI. EXTERNAL RISK MITIGATION POLICIES:

Firewall protection, operating system security patches, and software products shall be reasonably up-to-date and installed on any HSS computer that stores or processes personal information.

Personal information 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.

All system security software including, anti-virus, anti-malware, and internet security shall be reasonably up-to-date and installed on any HSS computer that stores or processes personal information.

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.

VII. OPERATIONAL PROTOCOL:

The Operational Protocol is effective June 1, 2015 and shall be reviewed and modified as deemed necessary at a meeting of the Data Security Coordinator and personnel responsible and/or authorized for the security of personal information. 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 WISP. At the time of publication, a copy of the WISP shall be distributed to all current HSS employees and to new hires on their date of employment.

A. 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.

Within 90 days of the publication of the WISP 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 personal information, assign those files to the appropriate secured storage location, and to redact, expunge or otherwise eliminate all unnecessary personal information in a manner consistent with the WISP.

Any personal information 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 WISP.

Any paper files containing personal information 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 personal information in their work area when they are not present (e.g., lunch breaks).
Paper or electronically stored records containing personal information 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 personal information 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 personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

Electronic records containing personal information 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 personal information or it is technologically not feasible to encrypt the data as and where transmitted.

If necessary for the functioning of individual departments, the department head, in consultation with the Data Security Coordinator or his/her designee(s), may develop departmental rules that ensure reasonable restrictions upon access and handling of files containing personal information and must comply with all WISP standards. Departmental rules are to be published as an addendum to the WISP.

B. Access Control Protocol:

All HSS computers shall restrict user access to those employees having an authorized and unique log-in ID.

All computers that have been inactive for 20 or more minutes shall require re-log-in.
After 5 unsuccessful log-in attempts by any user ID, that user ID will be blocked from accessing any computer or file stored on any computer until access privileges are reestablished by the Data Security Coordinator or his/her designee(s); which may include Corporate IT.

Access to electronically stored records containing personal information shall be electronically limited to those employees having an authorized and unique log-in ID assigned by the Data Security Coordinator or his/her designee(s); which may include Corporate IT.

Where practical, all visitors who are expected to access areas other than common space or are granted access to office space containing personal information should be required to sign-in.

Where practical, all visitors are restricted from areas where files containing personal information are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files containing personal information are stored.

All computers with an internet connections or any HSS computer that stores or processes personal information must have a reasonably up-to-date version of software providing virus, anti-spyware and anti-malware protection installed and active at all times.

C. 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 personal information ("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 signed on or after June 1, 2015 with a Third Party Service Provider who will have access to the personal information of end-users shall require the Service Provider to implement security standards consistent the security protocols defined in this WISP.

(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 WISP.

VIII. Breach of Data Security Protocol:

Should any employee know of a security breach at any of HSS' facilities, or that any unencrypted personal information has been lost or stolen or accessed without authorization, or that encrypted personal information along with the access code or security key has been acquired by an unauthorized person or for an unauthorized purpose, the following protocol is to be followed:

(a) Employees are to notify the Data Security Coordinator or the employee's manager in the event of a known or suspected security breach or unauthorized use of personal information. The Data Security Coordinator and manager must then report any such known or suspected breach or unauthorized use to their Executive Vice President who shall also ensure that the Data Security Coordinator is aware of the suspected breach or unauthorized use.

(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 breach or unauthorized acquisition or use of personal information;
(2) The number of applicable personsaffected 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.

Harris School Solutions
Written Information Security Plan (WISP)

Table of Contents

I. OBJECTIVE:

The objective of Harris School Solutions (HSS) in the development and implementation of this comprehensive written information security program ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of personal information (personally identifiable information "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 any applicable laws or regulations (the "regulations").

The WISP sets forth our procedure for evaluating and addressing our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of all end users.

For purposes of this WISP, the term "Student Data" means personally identifiable information from student records that Third Party Contractor receives from a School District. The term "Teacher or Principal Data" shall mean personally identifiable information from the records of a School District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release. "Personally Identifiable Information" ("PII") as applied to Student Data, means personally identifiable information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA), at 20 USC 1232g.

II. PURPOSE:

The purpose of the WISP is to better: (a) ensure the security and confidentiality of Student Data, Teacher or Principal data and other personal information, (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.

III. SCOPE:

In formulating and implementing the WISP, Harris School Solutions 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 personal information;

(b) assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;

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

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

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

IV. DATA SECURITY COORDINATOR:

Harris School Solutions has designated a Data Security Coordinator to implement, supervise and maintain the WISP. The Data Security Coordinator may be an individual and / or may also be comprised of one or more members of the Corporate IT staff and shall be responsible for the following:

(a) Implementation of the WISP including all provisions outlined in Section VII of this policy: Daily Operational Protocol;

(b) Training of all employees;

(c) Regular testing of the WISP's safeguards;

(d) Evaluating the ability of any of our third party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access, and requiring such third party service providers by contract to implement and maintain appropriate security measures;

(e) Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information; and

(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 personal information on the elements of the WISP.

V. INTERNAL RISK MITIGATION POLICIES:

To guard against internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, 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.

(b) Access to records containing personal information 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.

(c) Written and electronic records containing personal information shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements. HSS' frequent business records needs and associated retention and secure destruction periods are set at three (3) years.

(d) A copy of the WISP is to be distributed to each current Harris HSS employee and to each new employee on the beginning date of their employment. Employees are encouraged and invited to advise their manager or the Data Security Coordinator of any activities or operations which appear to pose risks to the security of personal information.

(e) Internal HSS training session for all current HSS employees will be held during the first-half of 2016 to detail the provisions of the WISP, and as otherwise as detailed in this policy.

(f) Terminated employees must return all records containing personal data, 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.

(g) A terminated employee's physical and electronic access to records containing personal information shall be restricted 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.

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

(i) All security measures including the WISP shall be reviewed annually in the first quarter of each such year to ensure that the policies contained in the WISP are adequate to meet all applicable regulations.

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

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

(l) If applicable, the Data Security Coordinator or his/her designee(s) shall maintain a secured and confidential master list of all lock combinations, passwords, and keys. The list will identify which employees possess keys, keycards, or other access devices and that only approved employee have been provided access credentials.

(m)The Data Security Coordinator or his/her designee(s) shall ensure that access to personal information in restricted to approved and active user accounts.

(n) Current employees' user ID's and passwords shall conform to accepted security standards. All passwords shall be changed at least annually, or more often as needed (e.g. seasonally).

(o) Employees are required to report suspicious or unauthorized use of personal information to a supervisor, the Data Security Coordinator or his/her designee(s).

(p) Whenever there is an incident that requires notification pursuant to any 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 personal information.

VI. EXTERNAL RISK MITIGATION POLICIES:

Firewall protection, operating system security patches, and software products shall be reasonably up-to-date and installed on any HSS computer that stores or processes personal information.

Personal information 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.

All system security software including, anti-virus, anti-malware, and internet security shall be reasonably up-to-date and installed on any HSS computer that stores or processes personal information.

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.

VII. OPERATIONAL PROTOCOL:

The Operational Protocol is effective June 1, 2015 and shall be reviewed and modified as deemed necessary at a meeting of the Data Security Coordinator and personnel responsible and/or authorized for the security of personal information. 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 WISP. At the time of publication, a copy of the WISP shall be distributed to all current HSS employees and to new hires on their date of employment.

A. 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.

Within 90 days of the publication of the WISP 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 personal information, assign those files to the appropriate secured storage location, and to redact, expunge or otherwise eliminate all unnecessary personal information in a manner consistent with the WISP.

Any personal information 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 WISP.

Any paper files containing personal information 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 personal information in their work area when they are not present (e.g., lunch breaks).
Paper or electronically stored records containing personal information 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 personal information 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 personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

Electronic records containing personal information 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 personal information or it is technologically not feasible to encrypt the data as and where transmitted.

If necessary for the functioning of individual departments, the department head, in consultation with the Data Security Coordinator or his/her designee(s), may develop departmental rules that ensure reasonable restrictions upon access and handling of files containing personal information and must comply with all WISP standards. Departmental rules are to be published as an addendum to the WISP.

B. Access Control Protocol:

All HSS computers shall restrict user access to those employees having an authorized and unique log-in ID.

All computers that have been inactive for 20 or more minutes shall require re-log-in.
After 5 unsuccessful log-in attempts by any user ID, that user ID will be blocked from accessing any computer or file stored on any computer until access privileges are reestablished by the Data Security Coordinator or his/her designee(s); which may include Corporate IT.

Access to electronically stored records containing personal information shall be electronically limited to those employees having an authorized and unique log-in ID assigned by the Data Security Coordinator or his/her designee(s); which may include Corporate IT.

Where practical, all visitors who are expected to access areas other than common space or are granted access to office space containing personal information should be required to sign-in.

Where practical, all visitors are restricted from areas where files containing personal information are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files containing personal information are stored.

All computers with an internet connections or any HSS computer that stores or processes personal information must have a reasonably up-to-date version of software providing virus, anti-spyware and anti-malware protection installed and active at all times.

C. 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 personal information ("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 signed on or after June 1, 2015 with a Third Party Service Provider who will have access to the personal information of end-users shall require the Service Provider to implement security standards consistent the security protocols defined in this WISP.

(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 WISP.

VIII. Breach of Data Security Protocol:

Should any employee know of a security breach at any of HSS' facilities, or that any unencrypted personal information has been lost or stolen or accessed without authorization, or that encrypted personal information along with the access code or security key has been acquired by an unauthorized person or for an unauthorized purpose, the following protocol is to be followed:

(a) Employees are to notify the Data Security Coordinator or the employee's manager in the event of a known or suspected security breach or unauthorized use of personal information. The Data Security Coordinator and manager must then report any such known or suspected breach or unauthorized use to their Executive Vice President who shall also ensure that the Data Security Coordinator is aware of the suspected breach or unauthorized use.

(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 breach or unauthorized acquisition or use of personal information;
(2) The number of applicable personsaffected 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.