UNION SPRINGS
CENTRAL SCHOOL DISTRICT

Union Springs Central School District

239 Cayuga Street
Union Springs, NY 12160

Phone: 315-889-4105   www.unionspringscsd.org   Fax: 315-889-4108

August 1st, 2022

Dear Customer Service,

New York State added new regulations to enforce New York State Ed Law 2-D
(https://www.nysenate.gov/legislation/laws/EDN/2-D).

"The Board of Regents adopted Part 121 of the Regulations of the Commissioner of Education on January 13, 2020. These rules will implement Education Law Section 2-d and provide guidance to educational agencies and their third-party contractors on ways to strengthen data privacy and security to protect student data and annual professional performance review data."

As a result, all New York State public schools are required to post the vendor contract between each district and the vendor. There are multiple signatures and a summary on how you handle our data required throughout this document.

If we are unable to receive these documents signed by you, we will not be able to provide this resource to students and teachers. If you have any questions you may contact me directly.

Thank You,

Kevin Casler
Chief Technology Officer
Union Springs Central School
kcasler@unionspringscsd.org
(315) 889-4105

UNION SPRINGS
CENTRAL SCHOOL DISTRICT

Union Springs Central School District

239 Cayuga Street
Union Springs, NY 12160

Phone: 315-889-4105   www.unionspringscsd.org   Fax: 315-889-4108

DATA SHARING AND CONFIDENTIALITY AGREEMENT

Including

Union Springs Central School District Bill of Rights for Data Security and Privacy and
Supplemental Information about a Master Agreement between Union
Springs Central School District and   Impero Solutions Inc.

ADDENDUM A Parent's Bill of Rights for Data Privacy and Security

The Union Springs Central School District is committed to ensuring student privacy in accordance with local, state and federal regulations. Pursuant to the New York State Education Law 2-D, the district is providing the following Parents' Bill of Rights for Data Privacy and Security:

1.   A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and FERPA, includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2.   The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to parents of an Eligible Student.

3.   State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99);
Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4.   Safeguards associated with industry standards and best practices including but not limited to encryption, firewalls and password protection must be in place when student PII is stored or transferred.

UNION SPRINGS

Union Springs Central School District

239 Cayuga Street
Union Springs, NY 12160
Phone: 315-889-4105   www.unionspringscsd.org   Fax: 315-889-4108

---

5. A complete list of all student data elements collected by NYSED is available at http://www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. Complaints may be submitted to NYSED at http://www.nysed.gov/data-privacy- security/report- improper disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 WashingtonAvenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474- 0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

10. Parents have the right to submit complaints about possible breaches of student data. Any such complaint must be submitted in writing to:

Jarett S. Powers, Ed.D., Superintendent of Schools Union Springs Central School District 239
Cayuga St.
Union Springs, NY 13160

Supplemental Information About Third Party Contracts

In order to meet 21st century expectations for effective education and efficient operation, the district utilizes several products and services that involve third party vendors receiving access to student data protected by Section 2-d of the Education Law. The District recognizes that students, parents, and the school community have a legitimate interest in understanding which of the district's vendors receive that data, for what purpose, and under what conditions. The district has undertaken the task of compiling that information, and of ensuring that each new contract adequately describes (1) the exclusive purposes for which the data will be used, (2) how the vendor will ensure that any subcontractors it uses will abide by data protection and security requirements, (3) when the contract expires and what happens to the data at that time, (4) if and how an affected party can challenge the accuracy of the data that is collected, (5) where the data will be stored, and (6) the security protections taken to ensure the data will be protected, including whether the data will be encrypted.

Adoption Date 10/26/2020

UNION SPRINGS
CENTRAL SCHOOL DISTRICT

Union Springs Central School District

239 Cayuga Street
Union Springs, NY 12160

Phone: 315-889-4105   www.unionspringscsd.org   Fax: 315-889-4108

As required by law by Education Law Section 2-D the Parent's Bill of Rights for Data Privacy and Security has been included in this Data Sharing and Confidentiality Agreement. Vendor shall complete and that they have read and agree to terms and to append it to this Data Sharing and Confidentiality Agreement. BY THE VENDOR:

Steve Stolfi	08 August 2024 | 6:46 PM BST
Name (Print)	Date

CCO

Title

DocuSigned by:

Steve Stolfi

D6ED6993D9DA4CE...

Signature

UNION SPRINGS

Union Springs Central School District

239 Cayuga Street
Union Springs, NY 12160
Phone: 315-889-4105   www.unionspringscsd.org   Fax: 315-889-4108

ADDENDUM B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PII

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Contract End Date	See applicable order
Subcontractor Written Agreement Requirement (Specify if the contractor will utilize sub-contractors and how it will manage sub-contractor relationships and contracts)	See Terms & Conditions https://www.imperosoftware.com/policies-terms/ with sub-processor list https://www.imperosoftware.com/wp-content/uploads/2021/06/Data-Processor-List-2021-02-22.pdf
Data Transition and Secure Destruction (Describe whether, how and when data will be returned or destroyed when the contract is terminated)	Upon expiration or termination of the Contract, Contractor shall: See Terms & Conditions https://www.imperosoftware.com/policies-terms/
Data Accuracy	See Terms & Conditions https://www.imperosoftware.com/policies-terms/

UNION SPRINGS
CENTRAL SCHOOL DISTRICT

Union Springs Central School District

239 Cayuga Street
Union Springs, NY 12160

Phone: 315-889-4105   www.unionspringscsd.org   Fax: 315-889-4108

Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: See Terms & Conditions https://www.imperosoftware.com/policies-terms/

ADDENDUM C

District Data Privacy and Security Policy

The District is committed to maintaining the privacy and security of student data and teacher and principal data and will follow all applicable laws and regulations for the handling and storage of this data in the District and when disclosing or releasing it to others, including, but not limited to, third-party contractors. The District adopt this policy to implement the requirements of Education Law Section 2-d and its implementing regulations, as well as to align the District's data privacy and security practices with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

Definitions

As provided in Education Law Section 2-d and/or its implementing regulations, the following terms, as used in this policy, will mean:

a)   "Breach" means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.

b)   "Building principal" means a building principal subject to annual performance evaluation review under the provisions of Education Law Section 3012-c.

UNION SPRINGS

Union Springs Central School District

239 Cayuga Street
Union Springs, NY 12160

Phone: 315-889-4105   www.unionspringscsd.org   Fax: 315-889-4108

---

c)   "Classroom teacher" means a teacher subject to annual performance evaluation review under the provisions of Education Law Section 3012-c.

d)   "Commercial or marketing purpose" means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve, or market products or services to students.

e)   "Contract or other written agreement" means a binding agreement between an educational agency and a third-party, which includes, but is not limited to, an agreement created in electronic form and signed with an electronic or digital signature or a click-wrap agreement that is used with software licenses, downloaded, and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.

f)   "Disclose" or "disclosure" means to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.

g)   "Education records" means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.

h)   "Educational agency" means a school district, board of cooperative educational services (BOCES), school, or the New York State Education Department (NYSED).

i)   "Eligible student" means a student who is eighteen years or older.

j)   "Encryption" means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States Department of Health and Human Services in guidance issued under 42 USC Section 17932(h)(2).

k)   "FERPA" means the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.

l)   "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). A copy of the NIST Cybersecurity Framework is available at the Office of Counsel, State Education Department, State Education Building, Room 148, 89 Washington Avenue, Albany, New York 12234.

m)   "Parent" means a parent, legal guardian, or person in parental relation to a student.

n)   "Personally identifiable information (PII)," as applied to student data, means personally identifiable information as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act, 20 USC Section 1232g, and, as applied to teacher or principal data, means personally identifying information as this term is defined in Education Law Section 3012-c(10).

o)   "Release" has the same meaning as disclosure or disclose.

p)   "Student" means any person attending or seeking to enroll in an educational agency.

q)   "Student data" means personally identifiable information from the student records of an educational agency.

r)   "Teacher or principal data" means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law Sections 3012-c and 3012d.

s)   "Third-party contractor" means any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to the educational agency, including but not limited to data management or storage services, conducting studies for or on behalf ofthe educational agency, or audit or evaluation of publicly funded programs. This term will include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities pursuant to Education Law Section 211-e and is not an educational agency, and a not- for-profit corporation or other nonprofit organization, other than an educational agency.

t)   "Unauthorized disclosure" or "unauthorized release" means any disclosure or release not permitted by federal or state statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

Data Collection Transparency and Restrictions

As part of its commitment to maintaining the privacy and security of student data and teacher and principal data, the District will take steps to minimize its collection, processing, and transmission of PII. Additionally, the District will:

a)   Not sell PII nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

Union Springs Central School District

239 Cayuga Street
Union Springs, NY 12160

Phone: 315-889-4105   www.unionspringscsd.org   Fax: 315-889-4108

b)   Ensure that it has provisions in its contracts with third-party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with law, regulation, and District policy.

Except as required by law or in the case of educational enrollment data, the District will not report to NYSED the following student data elements:

a)   Juvenile delinquency records;

b)   Criminal records;

c)   Medical and health records; and

d)   Student biometric information.

Nothing in Education Law Section 2-d or this policy should be construed as limiting the administrative use of student data or teacher or principal data by a person acting exclusively in the person's capacity as an employee of the District.

Chief Privacy Officer

The Commissioner of Education has appointed a Chief Privacy Officer who will report to the Commissioner on matters affecting privacy and the security of student data and teacher and principal data. Among other functions, the Chief Privacy Officer is authorized to provide assistance to educational agencies within the state on minimum standards and best practices associated with privacy and the security of student data and teacher and principal data.

The District will comply with its obligation to report breaches or unauthorized releases of student data or teacher or principal data to the Chief Privacy Officer in accordance with Education Law Section 2-d, its implementing regulations, and this policy.

The Chief Privacy Officer has the power, among others, to:

a)   Access all records, reports, audits, reviews, documents, papers, recommendations, and other materials maintained by the District that relate to student data or teacher or principal data, which includes, but is not limited to, records related to any technology product or service that will be utilized to store and/or process PII; and

b)   Based upon a review of these records, require the District to act to ensure that PII is protected in accordance with laws and regulations, including but not limited to requiring the District to perform a privacy impact and security risk assessment.

Data Protection Officer

The District has designated a District employee to serve as the District's Data Protection Officer. *The Data Protection Officer for the District is Catherine Cahill.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the District.

The District will ensure that the Data Protection Officer has the appropriate knowledge, training, and experience to administer these functions. The Data Protection Officer may perform these functions in addition to other job responsibilities. Additionally, some aspects of this role may be outsourced to a provider such as a BOCES, to the extent available.

District Data Privacy and Security Standards

The District will use the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1) (Framework) as the standard for its data privacy and security program. The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. The Framework provides a common taxonomy and mechanism for organizations to:

a)   Describe their current cybersecurity posture;

b)   Describe their target state for cybersecurity;

c)   Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;

d)   Assess progress toward the target state; and

e)   Communicate among internal and external stakeholders about cybersecurity risk.

UNION SPRINGS

Union Springs Central School District

239 Cayuga Street
Union Springs, NY 12160
Phone: 315-889-4105   www.unionspringscsd.org   Fax: 315-889-4108

The District will protect the privacy of PII by:

a)   Ensuring that every use and disclosure of PII by the District benefits students and the District by considering, among other criteria, whether the use and/or disclosure will:

1.   Improve academic achievement;

2.   Empower parents and students with information; and/or

3.   Advance efficient and effective school operations.

b)   Not including PII in public reports or other public documents.

The District affords all protections under FERPA and the Individuals with Disabilities Education Act and their implementing regulations to parents or eligible students, where applicable.

Third-Party Contractors

District Responsibilities

The District will ensure that whenever it enters into a contract or other written agreement with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the District, the contract or written agreement will include provisions requiring that confidentiality of shared student data or teacher or principal data be maintained in accordance with law, regulation, and District policy.

In addition, the District will ensure that the contract or written agreement includes the third-party contractor's data privacy and security plan that has been accepted by the District.

The third-party contractor's data privacy and security plan must, at a minimum:

a)   Outline how the third-party contractor will implement all state, federal, and local data privacy and security contract requirements over the life of the contract, consistent with District policy;

b)   Specify the administrative, operational, and technical safeguards and practices the third-party contractor has in place to protect PII that it will receive under the contract;

c)   Demonstrate that the third-party contractor complies with the requirements of 8 NYCRR Section 121.3(c);

d)   Specify how officers or employees of the third-party contractor and its assignees who have access to student data or teacher or principal data receive or will receive training on the laws governing confidentiality of this data prior to receiving access;

e)   Specify if the third-party contractor will utilize subcontractors and how it will manage those relationships and contracts to ensure PII is protected;

f)   Specify how the third-party contractor will manage data privacy and security incidents that implicate PII including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District;

g)   Describe whether, how, and when data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires; and

h)   Include a signed copy of the Parents' Bill of Rights for Data Privacy and Security.

Third-Party Contractor Responsibilities

Each third-party contractor, that enters into a contract or other written agreement with the District under which the third-party contractor will receive student data or teacher or principal data from the District, is required to:

a)   Adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework;

b)   Comply with District policy and Education Law Section 2-d and its implementing regulations;

c)   Limit internal access to PII to only those employees or subcontractors that have legitimate educational interests (i.e., they need access to provide the contracted services);

d)   Not use the PII for any purpose not explicitly authorized in its contract;

---

e)   Not disclose any PII to any other party without the prior written consent of the parent or eligible student:

1.   Except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with law, regulation, and its contract with the District; or

2.   Unless required by law or court order and the third-party contractor provides a notice of the disclosure to NYSED, the Board, or the institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by law or court order;

f)   Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII in its custody;

g)   Use encryption to protect PII in its custody while in motion or at rest; and

h)   Not sell PII nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

Where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by law and contract apply to the subcontractor.

Cooperative Educational Services through a BOCES

The District may not be required to enter into a separate contract or data sharing and confidentiality agreement with a third-party contractor that will receive student data or teacher or principal data from the District under all circumstances.

For example, the District may not need its own contract or agreement where:

a)   It has entered into a cooperative educational service agreement (CoSer) with a BOCES that includes use of a third-party contractor's product or service; and

b)   That BOCES has entered into a contract or data sharing and confidentiality agreement with the third-party contractor, pursuant to Education Law Section 2-d and its implementing regulations, that is applicable to the District's use of the product or service under that CoSer.

To meet its obligations whenever student data or teacher or principal data from the District is received by a third-party contractor pursuant to a CoSer, the District will consult with the BOCES to, among other things:

a)   Ensure there is a contract or data sharing and confidentiality agreement pursuant to Education Law Section 2-d and its implementing regulations in place that would specifically govern the District's use of a third-party contractor's product or service under a particular CoSer;

b)   Determine procedures for including supplemental information about any applicable contracts or data sharing and confidentiality agreements that a BOCES has entered into with a third-party contractor in its Parents' Bill of Rights for Data Privacy and Security;

c)   Ensure appropriate notification is provided to affected parents, eligible students, teachers, and/or principals about any breach or unauthorized release of PII that a third-party contractor has received from the District pursuant to a BOCES contract; and

d)   Coordinate reporting to the Chief Privacy Officer to avoid duplication in the event the District receives information directly from a third-party contractor about a breach or unauthorized release of PII that the third-party contractor received from the District pursuant to a BOCES contract.

Click-Wrap Agreements

Periodically, District staff may wish to use software, applications, or other technologies in which the user must "click" a button or box to agree to certain online terms of service prior to using the software, application, or other technology. These are known as "click-wrap agreements" and are considered legally binding "contracts or other written agreements" under Education Law Section 2-d and its implementing regulations.

District staff are prohibited from using software, applications, or other technologies pursuant to a clickwrap agreement in which the third-party contractor receives student data or teacher or principal data from the District unless they have received prior approval from the District's Data Privacy Officer or designee.

The District will develop and implement procedures requiring prior review and approval for staff use of any software, applications, or other technologies pursuant to click-wrap agreements.

Parents' Bill of Rights for Data Privacy and Security

The District will publish its Parents' Bill of Rights for Data Privacy and Security (Bill of Rights) on its website. Additionally, the District will include the Bill of Rights with every contract or other written agreement it

enters into with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the district.

The Bill of Rights will contain all required elements including supplemental information for each contract the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District. The supplemental information must be developed by the District and include the following information:

a)   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;

b)   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);

c)   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 District, and/or whether, when, and how the data will be destroyed);

d)   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;

e)   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; and

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

The District will publish on its website the supplement to the Bill of Rights (i.e., the supplemental information described above) for any contract or other written agreement it has entered into with a third-party contractor that will receive PII from the District. The Bill of Rights and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the District's data and/or technology infrastructure.

UNION SPRINGS

Union Springs Central School District

239 Cayuga Street
Union Springs, NY 12160
Phone: 315-889-4105   www.unionspringscsd.org   Fax: 315-889-4108

Right of Parents and Eligible Students to Inspect and Review Students' Education Records

Consistent with the obligations of the District under FERPA, parents and eligible students have the right to inspect and review a student's education record by making a request directly to the District in a manner prescribed by the District.

The District will ensure that only authorized individuals are able to inspect and review student data. To that end, the District will take steps to verify the identity of parents or eligible students who submit requests to inspect and review an education record and verify the individual's authority to do so.

Requests by a parent or eligible student for access to a student's education records must be directed to the District and not to a third-party contractor. The District may require that requests to inspect and review education records be made in writing.

The District will notify parents annually of their right to request to inspect and review their child's education record including any student data stored or maintained by the District through its annual FERPA notice. A notice separate from the District's annual FERPA notice is not required.

The District will comply with a request for access to records within a reasonable period, but not more than 45 calendar days after receipt of a request.

The District may provide the records to a parent or eligible student electronically, if the parent consents. The District must transmit the PII in a way that complies with laws and regulations. Safeguards associated with industry standards and best practices, including but not limited to encryption and password protection, must be in place when education records requested by a parent or eligible student are electronically transmitted.

Complaints of Breach or Unauthorized Release of Student Data and/or Teacher or Principal Data

The District will inform parents, through its Parents' Bill of Rights for Data Privacy and Security, that they have the right to submit complaints about possible breaches of student data to the Chief Privacy Officer at NYSED. In addition, the District has established the following procedures for parents, eligible students, teachers, principals, and other District staff to file complaints with the District about breaches or unauthorized releases of student data and/or teacher or principal data:

a)   All complaints must be submitted to the District's Data Protection Officer in writing.

b)   Upon receipt of a complaint, the District will promptly acknowledge receipt of the complaint, commence an investigation, and take the necessary precautions to protect PII.

c)   Following the investigation of a submitted complaint, the District will provide the individual who filed the complaint with its findings. This will be completed within a reasonable period of time, but no more than 60 calendar days from the receipt of the complaint by the District.

d)   If the District requires additional time, or where the response may compromise security or impede a law enforcement investigation, the District will provide the individual who filed the complaint with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint.

These procedures will be disseminated to parents, eligible students, teachers, principals, and other District staff.

The District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies.

Reporting a Breach or Unauthorized Release

The District will report every discovery or report of a breach or unauthorized release of student data or teacher or principal data within the District to the Chief Privacy Officer without unreasonable delay, but no more than ten calendar days after the discovery.

Each third-party contractor that receives student data or teacher or principal data pursuant to a contract or other written agreement entered into with the District will be required to promptly notify the District of any breach of security resulting in an unauthorized release of the data by the third-party contractor or its assignees in violation of applicable laws and regulations, the Parents' Bill of Rights for Student Data Privacy and Security, District policy, and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay, but no more than seven calendar days after the discovery of the breach.

In the event of notification from a third-party contractor, the District will in turn notify the Chief Privacy Officer of the breach or unauthorized release of student data or teacher or principal data no more than ten calendar days after it receives the third-party contractor's notification using a form or format prescribed by NYSED.

Investigation of Reports of Breach or Unauthorized Release by the Chief Privacy Officer

The Chief Privacy Officer is required to investigate reports of breaches or unauthorized releases of student data or teacher or principal data by third-party contractors. As part of an investigation, the Chief Privacy Officer may require that the parties submit documentation, provide testimony, and may visit, examine, and/or inspect the third-party contractor's facilities and records.

UNION SPRINGS

Union Springs Central School District

239 Cayuga Street
Union Springs, NY 12160

Phone: 315-889-4105   www.unionspringscsd.org   Fax: 315-889-4108

Upon the belief that a breach or unauthorized release constitutes criminal conduct, the Chief Privacy Officer is required to report the breach and unauthorized release to law enforcement in the most expedient way possible and without unreasonable delay.

Third-party contractors are required to cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of PII.

Upon conclusion of an investigation, if the Chief Privacy Officer determines that a third-party contractor has through its actions or omissions caused student data or teacher or principal data to be breached or released to any person or entity not authorized by law to receive this data in violation of applicable laws and regulations, District policy, and/or any binding contractual obligations, the Chief Privacy Officer is required to notify the third-party contractor of the finding and give the third-party contractor no more than 30 days to submit a written response.

If after reviewing the third-party contractor's written response, the Chief Privacy Officer determines the incident to be a violation of Education Law Section 2-d, the Chief Privacy Officer will be authorized to:

a)   Order the third-party contractor be precluded from accessing PII from the affected educational agency for a fixed period of up to five years;

b)   Order that a third-party contractor or assignee who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data be precluded from accessing student data or teacher or principal data from any educational agency in the state for a fixed period of up to five years;

c)   Order that a third-party contractor who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data will not be deemed a responsible bidder or offe\ror on any contract with an educational agency that involves the sharing of student data or teacher or principal data, as applicable for purposes of General Municipal Law Section 103 or State Finance Law Section 163(10)(c), as applicable, for a fixed period of up to five years; and/or

d)   Require the third-party contractor to provide additional training governing confidentiality of student data and/or teacher or principal data to all its officers and employees with reasonable access to this data and certify that the training has been performed at the contractor's expense. This additional training is required to be performed immediately and include a review of laws, rules, and regulations, including Education Law Section 2-d and its implementing regulations.

If the Chief Privacy Officer determines that the breach or unauthorized release of student data or teacher or principal data on the part of the third-party contractor or assignee was inadvertent and done without

intent, knowledge, recklessness, or gross negligence, the Chief Privacy Officer may make a recommendation to the Commissioner that no penalty be issued to the third-party contractor.

The Commissioner would then make a final determination as to whether the breach or unauthorized release was inadvertent and done without intent, knowledge, recklessness or gross negligence and whether or not a penalty should be issued.

Notification of a Breach or Unauthorized Release

The District will notify affected parents, eligible students, teachers, and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release of PII by the District or the receipt of a notification of a breach or unauthorized release of PII from a third-party contractor unless that notification would interfere with an ongoing investigation by law enforcement or cause further disclosure of PII by disclosing an unfixed security vulnerability. Where notification is delayed under these circumstances, the District will notify parents, eligible students, teachers, and/or principals within seven calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

Notifications will be clear, concise, use language that is plain and easy to understand, and to the extent available, include:

a)   A brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known;

b)   A description of the types of PII affected;

c)   An estimate of the number of records affected;

d)   A brief description of the District's investigation or plan to investigate; and

e)   Contact information for representatives who can assist parents or eligible students that have additional questions.
Notification will be directly provided to the affected parent, eligible student, teacher, or principal by first-class mail to their last known address, by email, or by telephone.

Where a breach or unauthorized release is attributed to a third-party contractor, the third-party contractor is required to pay for or promptly reimburse the District for the full cost of this notification.

Annual Data Privacy and Security Training

UNION SPRINGS

Union Springs Central School District

239 Cayuga Street
Union Springs, NY 12160

Phone: 315-889-4105   www.unionspringscsd.org   Fax: 315-889-4108

The District will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations. The District may deliver this training using online training tools. Additionally, this training may be included as part of the training that the District already offers to its workforce.

Notification of Policy

The District will publish this policy on its website and provide notice of the policy to all its officers and staff.

Education Law § 2-d
8 NYCRR Part 121

Adoption Date 10/26/2020

As required by law by Education Law Section 2-D District Data and Privacy and Security Policy has been included in this Data Sharing and Confidentiality Agreement. Vendor shall complete and that they have read and agree to terms and to append it to this Data Sharing and Confidentiality Agreement. Pursuant of Education Law Section 2-D the Educational Agency is required to post this completed Data Privacy Rider on their website.

BY THE VENDOR:

Steve Stolfi   CCO

_____   _____
Name (Print)   Title

DocuSigned by:

Steve Stolfi

D6ED6993D9DA4CE...
Signature   08 August 2024 | 6:46 PM BST

                                                    Date

UNION SPRINGS
Union Springs Central School District

239 Cayuga Street
Union Springs, NY 12160

Phone: 315-889-4105   www.unionspringscsd.org   Fax: 315-889-4108

DATA SHARING AND CONFIDENTIALITY AGREEMENT

1.   Purpose

(a)   Union Springs Central School District (hereinafter "USCSD") and [Name of Vendor] (hereinafter "Vendor") are parties to a contract or other written agreement pursuant to which Vendor will receive student data and/or teacher or principal data that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as "Section 2-d") from the District for purposes of providing certain products or services to the District (the "Master Agreement").

(b)   This Exhibit supplements the Master Agreement to which it is attached, to ensure that the Master Agreement conforms to the requirements of Section 2-d. This Exhibit consists of a Data Sharing and Confidentiality Agreement, a copy of the District's Bill of Rights for Data Security and Privacy signed by Vendor, and the Supplemental Information about the Master Agreement between USCSD and [Name of Vendor] that the District is required by Section 2-d to post on its website.

(c)   In consideration of the mutual promises set forth in the Master Agreement, Vendor agrees that it will comply with all terms set forth in the Master Agreement and this Exhibit. To the extent that any terms contained in the Master Agreement, or any terms contained in any other Exhibit(s) attached to and made a part of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.
In addition, in the event that Vendor has online or written Privacy Policies or Terms of Service (collectively, "TOS") that would otherwise be applicable to its customers or users of the products or services that are the subject of the Master Agreement between the District and Vendor, to the extent that any terms of the TOS, that are or may be in effect at any time during the term of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2.   Definitions

As used in this Exhibit:

(a)   "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor may receive from the District pursuant to the Master Agreement.

(b)   "Teacher or Principal Data" means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Vendor may receive from the District pursuant to the Master Agreement.

(c)   "Protected Data" means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service actually being provided to the District by Vendor pursuant to the Master Agreement.
(d)   "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

3.   Confidentiality of Protected Data

(a)   Vendor acknowledges that the Protected Data it receives pursuant to the Master Agreement originates from the District and that this Protected Data belongs to and is owned by the District.

(b)   Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and the District's policy on data security and privacy. The District will provide Vendor with a copy of its policy on data security and privacy upon request.

4.   Data Security and Privacy Plan

As more fully described herein, throughout the term of the Master Agreement, Vendor will have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from the District.

Vendor's Plan for protecting the District's Protected Data includes, but is not limited to, its agreement to comply with the terms of the District's Bill of Rights for Data Security and Privacy, a copy of which is set forth below and has been signed by the Vendor.

Additional components of Vendor's Data Security and Privacy Plan for protection of the District's Protected Data throughout the term of the Master Agreement are as follows:

(a)   Vendor will implement all state, federal, and local data security and privacy requirements including those contained within the Master Agreement and this Data Sharing and Confidentiality Agreement, consistent with the District's data security and privacy policy.

(b)   Vendor will have specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the District under the Master Agreement.

(c)   Vendor will comply with all obligations contained within the section set forth in this Exhibit below entitled "Supplemental Information about a Master Agreement between USCSD and [Name of Vendor]." Vendor's obligations described within this section include, but are not limited to:

(i)   its obligation to require subcontractors or other authorized persons or entities to whom it may disclose Protected Data (if any) to execute written agreements acknowledging that the data protection obligations imposed on Vendor by state and federal law and the Master Agreement shall apply to the subcontractor, and (ii) its obligation to follow certain procedures for the return, transition, deletion and/or destruction of Protected Data upon termination, expiration or assignment (to the extent authorized) of the Master Agreement.
(d)   Vendor has provided or will provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who will have access to Protected Data, prior to their receiving access.

(e)   Vendor will manage data security and privacy incidents that implicate Protected Data and will develop and implement plans to identify breaches and unauthorized disclosures. Vendor will provide prompt notification to the District of any breaches or unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement.

5.   <u>Notification of Breach and Unauthorized Release</u>

(a)   Vendor will promptly notify the District of any breach or unauthorized release of Protected Data it has received from the District in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.

(b)   Vendor will provide such notification to the District by contacting Jarett S. Powers, Ed.D., Superintendent of Schools directly by email at jpowers@unionspringscsd.org or by calling (315)889-4100.

(c)   Vendor will cooperate with the District and provide as much information as possible directly to Jarett S. Powers, Ed.D., Superintendent of Schools or his designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of Protected Data involved, an estimate of the number of records affected, the schools within the District affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d)   Vendor acknowledges that upon initial notification from Vendor, the District, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor agrees not to provide this notification to the CPO directly unless requested by the District or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by the District, Vendor will promptly inform Jarett S. Powers, Ed.D., Superintendent of Schools or his designee.

6.   <u>Additional Statutory and Regulatory Obligations</u>

Vendor acknowledges that it has the following additional obligations under Section 2-d with respect to any Protected Data received from the District, and that any failure to fulfill one or more of these statutory or regulatory obligations will be deemed a breach of the Master Agreement and the terms of this Data Sharing and Confidentiality Agreement:

(a)   To limit internal access to Protected Data to only those employees or subcontractors that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA); i.e., they need access in order to assist Vendor in fulfilling one or more of its obligations to the District under the Master Agreement.

(b)   To not use Protected Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and the Master Agreement to which this Exhibit is attached.

(c)   To not disclose any Protected Data to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations to the District and in compliance with state and federal law, regulations and the terms of the Master Agreement, unless:

(i)   the parent or eligible student has provided prior written consent; or

(ii)   the disclosure is required by statute or court order and notice of the disclosure is provided to the district no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order. (d) To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Data in its custody.

(e)   To use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

(f)   To adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.

(g)   To comply with the District's policy on data security and privacy, Section 2-d and Part 121.

(h)   To not sell Protected Data nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

(i)   To notify the District, in accordance with the provisions of Section 5 of this Data Sharing and Confidentiality Agreement, of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of applicable state or federal law, the District's Bill of Rights for Data Security and Privacy, the District's policies on data security and privacy, or other binding obligations relating to data privacy and security contained in the Master Agreement and this Exhibit. (j) To cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.

(k)   To pay for or promptly reimburse the District for the full cost of notification, in the event the District is required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

UNION SPRINGS

Union Springs Central School District

239 Cayuga Street
Union Springs, NY 12160
Phone: 315-889-4105   www.unionspringscsd.org   Fax: 315-889-4108

Supplemental Information about a Master Agreement between Union Springs Central School District and

The Union Springs Central School District has entered into a Master Agreement with **Name of Vendor**   ,
whichgoverns the availability to the District of the following products or services:

List specific product or services from Vendor here

Pursuant to the Master Agreement (which includes a Data Sharing and Confidentiality Agreement), the District
may provide to Vendor, and Vendor will receive, personally identifiable information about students and/or
teachers and principals that is protected by Section 2-d of the New York Education Law ("Protected Data").

Exclusive Purposes for which Protected Data will be Used: The exclusive purpose for which Vendor is receiving
Protected Data from the District is to provide the district with the functionality of the products or services listed
above. Vendor will not use the Protected Data for any other purposes not explicitly authorized above or within
the Master Agreement.

Oversight of Subcontractors: In the event that Vendor engages subcontractors or other authorized persons or
entities to perform one or more of its obligations under the Master Agreement (including subcontracting hosting
of the Protected Data to a hosting service provider), it will require those subcontractors or other authorized
persons or entities to whom it will disclose the Protected Data to execute legally binding agreements
acknowledging their obligation under Section 2-d of the New York Education Law to comply with all applicable
data protection, privacy and security requirements required of Vendor under the Master Agreement and
applicable state and federal law and regulations.

Duration of Agreement and Protected Data Upon Termination or Expiration:

- The Master Agreement commences on **Date**   and expires on **Date**   .
- Upon expiration of the Master Agreement without renewal, or upon termination of the Master
  Agreement prior to its expiration, Vendor will securely delete or otherwise destroy any and all Protected
  Data remaining in the possession of Vendor or any of its subcontractors or other authorized persons or
  entities to whom it has disclosed Protected Data. If requested by the District, Vendor will assist the
  District in exporting all Protected Data previously received back to the District for its own use, prior to
  deletion, in such formats as may be requested by the District.
- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the
  Master Agreement), the Vendor will cooperate with the District as necessary to transition Protected Data
  to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has
  disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected
  Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor
  and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected
  Data, as applicable, will provide the District with a certification from an appropriate officer that these
  requirements have been satisfied in full.

UNION SPRINGS   # Union Springs Central School District

239 Cayuga Street
Union Springs, NY 12160

Phone: 315-889-4105   www.unionspringscsd.org   Fax: 315-889-4108

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by the District to Vendor, by contacting the District regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may request to challenge the accuracy of APPR data provided to Vendor by following the appeal process in the District's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data that Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor (and, if applicable, its subcontractors) will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework, and safeguards associated with industry standards and best practices including, but not limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (and, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology that complies with Section 2-d of the New York Education Law.

UNION SPRINGS

Union Springs Central School District

239 Cayuga Street
Union Springs, NY 12160

Phone: 315-889-4105   www.unionspringscsd.org   Fax: 315-889-4108

In the event of a conflict between the terms of this Data Sharing and Confidentiality Agreement, Parent Bill of Rights and Data Security Privacy Plan, the terms of this Data Security and Privacy Plan shall control. All of the defined terms in the Agreement shall have the same definitions in the Data Security and Privacy Plan, unless otherwise defined herein. Except as expressly set forth in this Data Security and Privacy Plan, the terms and conditions of the Agreement shall remain unmodified and in full force and effect.

This agreement shall be published on the Union Springs Central School District website.

Vendor shall complete and acknowledge that they have read and agree to terms listed in the Data Sharing and Confidentiality Agreement.

IN WITNESS WHEREOF, the Contractor hereto has executed this agreement as of_____

DocuSigned by:

Steve Stolfi
D6ED6993D9DA4CE...

Signature

Steve Stolfi

Printed Name

CCO

Title

08 August 2024 | 6:46 PM BST

Date

By Union Springs Central School District

Signature

Kevin Casler

Printed Name

Chief Technology Officer

Title

Date

DocuSign

Certificate Of Completion

Envelope Id: 214A2CAC67364C18919CCB1008666F42   Status: Completed
Subject: Complete with Docusign: Ed Law 2D Contract Union Spring Central .docx
Source Envelope:
Document Pages: 27   Signatures: 3   Envelope Originator:
Certificate Pages: 4   Initials: 0   Impero Legal
AutoNav: Enabled   7th Floor, East West
EnvelopeId Stamping: Enabled   Tollhouse Hill
Time Zone: (UTC-08:00) Pacific Time (US & Canada)   Nottingham, NOTTINGHAM NG1 5FS
                                                             legal@imperosoftware.com
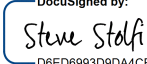   IP Address: 98.111.224.186

Record Tracking

Status: Original   Holder: Impero Legal   Location: DocuSign
        8/6/2024 5:09:59 PM   legal@imperosoftware.com

Signer Events	Signature	Timestamp
Steve Stolfi sstolfi@imperosoftware.com CCO Ativion Security Level: Email, Account Authentication (None)	DocuSigned by: *Steve Stolfi* D6ED6993D9DA4CE... Signature Adoption: Pre-selected Style Using IP Address: 172.59.9.78 Signed using mobile	Sent: 8/6/2024 5:16:08 PM Viewed: 8/8/2024 10:45:50 AM Signed: 8/8/2024 10:46:06 AM
Electronic Record and Signature Disclosure: Accepted: 8/8/2024 10:45:49 AM ID: 7283db06-02db-47d5-9890-683b6c5721ca Company Name: Impero Software		

In Person Signer Events	Signature	Timestamp

Editor Delivery Events	Status	Timestamp

Agent Delivery Events	Status	Timestamp

Intermediary Delivery Events	Status	Timestamp

Certified Delivery Events	Status	Timestamp

Carbon Copy Events	Status	Timestamp

Witness Events	Signature	Timestamp

Notary Events	Signature	Timestamp

Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	8/6/2024 5:16:09 PM
Certified Delivered	Security Checked	8/8/2024 10:45:50 AM
Signing Complete	Security Checked	8/8/2024 10:46:06 AM
Completed	Security Checked	8/8/2024 10:46:06 AM

Payment Events	Status	Timestamps

Electronic Record and Signature Disclosure

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, Impero Software (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a $0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact Impero Software:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:
To contact us by email send messages to: hrteam@imperosoftware.com

To advise Impero Software of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at hrteam@imperosoftware.com and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from Impero Software

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to and in the body of such request you must state your email address, full name, mailing address, and telephone number.

To withdraw your consent with Impero Software

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;

ii. send us an email to hrteam@imperosoftware.com and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: https://support.docusign.com/guides/signer-guide-signing-system-requirements.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify Impero Software as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by Impero Software during the course of your relationship with Impero Software.