

Central Islip Union Free School District

Program Information and Data Privacy

Third Party Agreement



To be completed **by the vendor** and submitted for all NEW and RENEWAL software/programs prior to purchase/implementation. Refusal of the vendor complete this agreement may serve as cause for the district to see similar services through another program and/or vendor. Failure to complete this form in its entirety will significantly delay any/all program purchases.

Software/Program Title:	Ecwid.com (freemium)
Publisher:	Lightspeed Commerce Inc.
Contract Pricing	<input type="checkbox"/> BOCES Contract or Shared Service <input type="checkbox"/> NYS Contract Pricing <input type="checkbox"/> Federal Contract Pricing <input type="checkbox"/> Direct Bid/RFP with Vendor <p style="text-align: right;"><u>NOT APPLICABLE</u></p>
Account Management	<input type="checkbox"/> SSO through LDAP/AD/ADFS/AZURE/SAML <input type="checkbox"/> SSO through Clever <input type="checkbox"/> NO SSO Option <input type="checkbox"/> Non SSO Centrally Managed (all Users) <input checked="" type="checkbox"/> <u>Non-User Based Program/Not Applicable</u>
Platform	<input type="checkbox"/> Local Install OR Device APP <input type="checkbox"/> Local Server/Network <input checked="" type="checkbox"/> <u>100% Web-based</u> <input type="checkbox"/> Web-Based with Local application/plugin <input type="checkbox"/> Other/Explain:
License Structure:	<input type="checkbox"/> Per-User <input type="checkbox"/> Per-Student <input type="checkbox"/> Per-Classroom <input type="checkbox"/> Per-Teacher <input type="checkbox"/> Per-Building <input type="checkbox"/> Districtwide/Unlimited <p style="text-align: right;"><u>NOT APPLICABLE</u></p>
License Renewal	<input checked="" type="checkbox"/> <u>Perpetual (no-renewal)</u> <input type="checkbox"/> Annual
Separate Hosting Fees:	<input checked="" type="checkbox"/> <u>NO</u> <input type="checkbox"/> YES - Annually <input type="checkbox"/> Other/Explain:

Adobe Flash	<input checked="" type="checkbox"/> <u>Program DOES NOT require Adobe Flash</u> <input type="checkbox"/> Program REQUIRES Adobe Flash Programs that still require Adobe Flash will not be considered for purchase or utilized
Configuration, Deployment, Initial Roll-Out Support	<input type="checkbox"/> Full On-Site Support Included in the Proposal/Fee <input type="checkbox"/> Remote Support Only <input type="checkbox"/> Remote Support Included/On-Site for Additional Fees <p style="text-align: center;"><u>NOT APPLICABLE</u></p>
Staff Training/Professional Development	<input type="checkbox"/> Full On-Site Training/Development Included in the Proposal/Fee <input type="checkbox"/> Remote/WebEx Training/Development and Support Only <input type="checkbox"/> Combined On-Site/WebEx Training included in proposal <p style="text-align: center;"><u>NOT APPLICABLE</u></p>
SIS-PowerSchool Integrations	<input type="checkbox"/> Program DOES NOT sync to SIS (PowerSchool) <input type="checkbox"/> Program DOES sync to SIS (PowerSchool) <p style="text-align: center;"><u>X Not Applicable</u></p>

ALL LINKS MUST BE PROVIDED AND COMPLETED BY THE VENDOR!

Software Title:	Ecwid.com (freemium)
Publisher/Developer:	Lightspeed Commerce Inc.
Developer/Vendor Name	Lightspeed Commerce Inc.
Developer/Vendor Mailing Address	700 St-Antoine St. E, Montreal QC, Canada H2Y 1A6
Developer/Vendor Privacy Policy Link:	https://www.lightspeedhq.com/legal/privacy-policy/
Developer/Vendor Parent Bill of Rights Link	https://www.lightspeedhq.com/legal/lightspeed-service-agreement/

EXHIBIT B

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).

Description of the purpose(s) for which Contractor will receive/access PII	Description: Student name to create account. <input type="checkbox"/> NO PII OR DATA IS COLLECTED OR VIEWABLE THROUGH THIS PROGRAM/APP
Type of PII that Contractor will receive/access	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> Employee PII
Contract Term	Each Contract is valid through the software renewal period or 3 school years in the case of "Free" programs, apps, extensions and pilots.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: <input type="checkbox"/> Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. <input checked="" type="checkbox"/> Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Encryption	<input checked="" type="checkbox"/> Data will be encrypted while in motion and at rest.


As the duly authorized officer of the "contractor" as listed above I attest to all of the above submitted information to be true and accept any liability and/or responsibility for any data breaches or intrusions associated with this program, applications, software or browser extension.

DocuSigned by:

AF631AEF86324F6...
Signature of Vendor Official Representative

12/20/2023
Date

Signature must be an actual signature and cannot be a script font or text. If the program does not collect or transmit any PII, this document must still be completed, initialed (pages) and signed but you may and the select "NO PII OR DATA IS COLLECTED OR VIEWABLE" option above. No program/app/extension will be considered without a complete agreement.

Contractor Initials: 

Data Processing Agreement

Data Processing Agreement

This Data Processing Agreement is by and between the Central Islip Union Free School District, an Educational Agency, and Lightspeed Commerce Inc.

1. About this DPA.

a) This Data Processing Agreement (“DPA”) is a legal agreement which forms an integral part of and applies in addition to the existing Lightspeed Service Agreement, Channel Partner Agreement, Reseller Partner Agreement or other written or electronic agreement between the parties (as applicable) (“Service Agreement”) concluded by and between the Customer (as defined in the Service Agreement) as controller and Lightspeed Commerce Inc. and the Lightspeed affiliate that is the contracting entity (as defined in the Service Agreement) (collectively referred to as “Lightspeed” in this DPA) as processors in connection with the provision of services, which include various data processing services, to Customer (“Services”). Signature of the Service Agreement shall be deemed to constitute signature and acceptance of this DPA, which is incorporated by reference therein.

b) This DPA consists of:

- the main body of the DPA
- Schedule 1. Description of Lightspeed’s Security Measures
- Schedule 2. *Only for Customers established in the European Economic Area (EEA), Switzerland or the UK*, the EU Standard Contractual Clauses for controller to processor (2021) are incorporated in this DPA by reference (“SCCs”). See Section 10 for more details about international data transfers.
- Schedule 3. *Only for Customers established in the United Kingdom (UK)*, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (version B1.0) is incorporated in this DPA by reference (“UK Addendum”) (*only available in English*).

2. Definitions.

Terms used in this DPA have the same meaning as those used in the Service Agreement, unless otherwise stated. If there are any conflicts or inconsistencies between the Service Agreement and this DPA, this DPA prevails.

3. Description of Personal Data.

When carrying out the Services, Lightspeed may have access to or otherwise receive or process information relating to identified or identifiable individuals (“Personal Data”).

a) **Type of Personal Data processed.** Depending on how the Customer chooses to use the Services, Lightspeed may process the following types of Personal Data:

First name, Last name; Contact information (e-mail address, home address, phone number); Language; Date of birth; IP address; Location data; Government-issued identification numbers; Financial information; Bank account details; Credit bureau reports (in the event Customer has subscribed to *Lightspeed Payments*).

Lightspeed may also process other kinds of Personal Data if Customer has chosen to collect and input such Personal Data into our Services. The Services do not require other kinds of Personal Data to function properly. Lightspeed disclaims all liability for damages or claims associated with Customer's choice to input non-compulsory Personal Data into the Services.

b) **Data subjects.** Personal Data about the following categories of individuals is processed:

- Owner(s) of a business that subscribes to Lightspeed's Services.
- Employees and other persons authorized by the Customer who have access to and use the Services (End-Users).
- Individuals whose Personal Data is processed using the Services, including a Customer's customers and suppliers.

4. Purposes of the processing.

Lightspeed is a provider of software as a service for point of sale solutions for the retail, golf, and hospitality industries, an online supplier network, as well as an online platform that can be used for eCommerce and related purposes. Lightspeed shall process Personal Data on behalf of the Customer to provide these services to the Customer pursuant to the Service Agreement and any additional purposes as instructed by Customer when using the Services. When Lightspeed acts as processor of the Personal Data, Lightspeed may only process Personal Data on behalf of Customer and solely for the purposes identified in this DPA and the Service Agreement.

5. Responsibilities regarding data processing.

a) **Controller.** Customer is the controller of all the Personal Data that it collects through the Services. Customer shall ensure that it is entitled to process and transfer the Personal Data to Lightspeed so that Lightspeed may lawfully process the Personal Data on Customer's behalf, as contemplated under this DPA.

b) **Processor.** Lightspeed acts as a processor of the Personal Data collected by the Customer through the use of the Services.

c) **Sub-processors.** Customer acknowledges and hereby grants its express written authorization that (i) Lightspeed's affiliates may act as Lightspeed's sub-processors; and (ii) Lightspeed may engage sub-processors as necessary to perform the Services. The list of Lightspeed's Authorized sub-processors can be found on [this webpage](#) and Customer acknowledges that these sub-processors are essential to provide the Services. Lightspeed will inform Customer if it adds, replaces or changes its sub-processors by updating the aforementioned list. Customer may object to the changes on legitimate grounds in accordance with the principles of good faith,

reasonableness and fairness within 30 calendar days after the change. Customer acknowledges that if it objects to Lightspeed's use of a sub-processor, Lightspeed will not be obligated to provide Customer the Services for which Lightspeed uses that sub-processor.

6. Data processing.

Lightspeed shall ensure that any processing shall be fair, lawful, and consistent with Lightspeed's obligations under this DPA and compliant with applicable data protection law. In particular,:

- a) **Controller instructions.** Lightspeed shall process Personal Data only on the documented instructions of Customer. If Lightspeed is required to additionally process Personal Data in compliance with an applicable law or regulation to which Lightspeed is subject, it will inform Customer of such legal requirement prior to such processing, unless prohibited from doing so by an applicable law or regulation;
- b) **Ensure appropriate protection.** Lightspeed shall ensure appropriate protection of Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where processing involves a transmission of Personal Data over a network, and against all other unlawful forms of processing;
- c) **Security safeguards.** Lightspeed shall comply with the security requirements set forth in Schedule 1, taking into consideration the state of the art, the costs of implementation and the nature, scope, context and purposes of processing;
- d) **Disclosure.** Lightspeed shall not disclose Personal Data to any third party or unauthorized persons, unless Customer has given its prior written consent to such disclosure and subject to the conditions laid down under section 6 of this DPA;
- e) **Confidentiality.** Lightspeed shall hold Personal Data in strict confidentiality and require that employees and any other person under its authority who will be provided access to or will otherwise process Personal Data are held to the same level of confidentiality in accordance with the requirements of the DPA (including during the term of their employment or engagement and thereafter);
- f) **Data subject requests.** Lightspeed shall take appropriate measures to assist the Customer, insofar as this is possible, in fulfilling Customer's obligations as a controller in responding to requests from individual data subjects to exercise their rights under any applicable data protection law or regulation. In addition, Lightspeed shall promptly notify Customer if it receives a request from an individual with respect to Personal Data, including but not limited to information access requests, information rectification requests, requests for blocking, erasure, or portability of Personal Data and shall not respond to any such requests unless expressly authorized to do so by Customer or unless required under an applicable data protection law or a law of the European Union or a Member State to which Lightspeed is subject; Additionally, Lightspeed shall ensure that it has implemented technical and organizational measures to assist Customer in fulfilling its obligation to respond to any such requests from an individual with respect to Personal Data processed.

Lightspeed shall promptly and properly deal with enquiries and requests from Customer in relation to the processing of Personal Data under this DPA;
- g) **Assistance with Customer's compliance.** Taking into account the nature of the processing and the information available to Lightspeed, Lightspeed shall assist the Customer in ensuring compliance with the obligations regarding security measures and conducting data protection impact assessments, where necessary pursuant to Articles 32-36 of the General Data Protection Regulation (GDPR).

Lightspeed shall assist and support Customer in the event of an investigation by a data protection authority or similar authority, if and to the extent that such investigation relates to the processing of Personal Data under this DPA.

Lightspeed shall promptly notify Customer if in Lightspeed's view an instruction given by Customer infringes applicable laws and regulations, including data protection laws, or a change in the applicable laws and regulations is likely to have a substantially adverse

effect on its ability to comply with its obligations under this DPA; Lightspeed shall be entitled to suspend the implementation of the instruction until a more lawful instruction is received. Lightspeed shall not carry out an instruction that is obviously unlawful;

This Data Processing Agreement is by and between the Central Islip Union Free School District, an Educational Agency, and Lightspeed Commerce Inc. of signature below.

h) **Disclosure requests.** To the extent permitted by applicable law, Lightspeed shall notify Customer of each request Lightspeed receives from a public authority requiring Lightspeed to disclose Personal Data processed in the context of the Service Agreement or to participate in an investigation involving that Personal Data. Lightspeed will make reasonable efforts to narrow the scope of any such request received and will provide only the Personal Data specifically requested;

i) **Data breach.** Lightspeed shall promptly (and in any event within forty-eight (48) hours) after becoming aware, notify Customer of any facts known to Lightspeed concerning any actual accidental or unauthorized access, disclosure or use, or accidental or unauthorized loss, damage or destruction of Personal Data by any current or former employee, contractor or agent of Lightspeed or by any other person or third party;

Lightspeed shall cooperate fully with Customer in the event of any accidental or unauthorized access, disclosure or use, or accidental or unauthorized loss, damage or destruction of Personal Data by any current or former employee, contractor or agent of Lightspeed or by any other person or third party, in order to limit the unauthorized disclosure or use, seek the return of any Personal Data, and assist in providing notice to competent regulators and affected individuals if requested by Customer.

7. Onward processing.

Lightspeed may only subcontract performance of part of the Services to third parties as subprocessors (including Lightspeed's affiliates outside the EEA, Switzerland and the UK) if Lightspeed ensures that such sub-processors are bound to obligations that are not less onerous than those set out in this DPA.

8. Retention and deletion.

a) Lightspeed processes Personal Data for as long as it is reasonably needed to deliver the Services. The retention term can be longer if Lightspeed is required to keep Personal Data longer on the basis of applicable law or to administer its business.

b) Upon request by Customer, Lightspeed shall immediately cease to process Personal Data and shall promptly return all such Personal Data, or delete the same, in accordance with such instructions as may be given by Customer at that time, unless it is required to store the Personal Data under an applicable law or regulation to which Lightspeed is subject or unless explicitly agreed otherwise with Customer. The obligations set out in this section shall remain in force notwithstanding termination or expiration of this DPA.

9. Audit and Compliance.

a) Lightspeed will make available to the Customer all information necessary to demonstrate compliance with the obligations regarding the processing of Personal Data provided to Lightspeed in its role as a data processor.

b) Lightspeed shall make the processing systems, facilities and supporting documentation relevant to the processing of Personal Data available for an audit by Customer or a qualified independent assessor selected by Customer and provide all assistance Customer may reasonably require for the audit no more than one time per 12-month period. If the audit demonstrates that Lightspeed has breached any obligation under the DPA, Lightspeed shall immediately cure that breach.

c) In case of inspection or audits by a competent governmental authority relating to the processing of Personal Data, Lightspeed shall make available its relevant processing systems, facilities and supporting documentation to the relevant competent public authority for an inspection or audit if this is necessary to comply with applicable laws. In the event of any inspection or audit, each party shall provide all reasonable assistance to the other party in responding to that inspection or audit. If a competent public authority deems the processing of Personal Data under this DPA unlawful, the parties shall take immediate action to ensure future compliance with applicable data protection law. Instead of on-site inspections and controls, Lightspeed may refer the Customer to an equivalent control by independent third parties (such as neutral data protection auditors), compliance with approved rules of conduct (Art. 40 GDPR) or suitable data protection or IT security certifications pursuant to Art. 42 GDPR. This applies in particular if company and business secrets of Lightspeed or Personal Data of third parties would be endangered by the controls.

d) Customer will reimburse Lightspeed for any reasonable costs incurred by Lightspeed in connection with any audit or inspection by (or on behalf of) Customer or a competent governmental authority, except where such audit or inspection reveals that Lightspeed has breached any of its obligations under the DPA.

e) Except where Lightspeed is otherwise prohibited by law from making such disclosure, Lightspeed shall promptly inform Customer if:

(i) it receives an inquiry, a subpoena or a request for inspection or audit from a competent public authority relating to the processing of Personal Data under this DPA, if it concerns the data of the Customer,; or (ii) it intends to disclose Personal Data to any competent public authority.

f) Lightspeed shall ensure that any employee, agent, independent contractor, or any other person engaging in the provision of the Services and who has access to Personal Data of Customer, shall comply with all data protection and privacy laws and regulations (including any and all legislative and/or regulatory amendments or successors thereto), applicable to Lightspeed.

10. Data transfers (only for Customers established in the EEA, Switzerland or the UK).

a) Customer authorizes Lightspeed to commission processing in a third country, including by sub-processors, if the specific requirements of articles 44-49 GDPR are met. Customer shall be deemed to have granted explicit consent for processing in a third country with regard to the processing operations by Lightspeed and the Authorized Sub-processors as listed [here](#).

b) Lightspeed Commerce Inc. is a company based in Canada. As such, most data transfers from Customers established in the European Economic Area (EEA), Switzerland or the United Kingdom (UK) to Lightspeed are made pursuant to the European Commission's [adequacy decision](#) for Canada.

c) To the extent that the adequacy decision does not apply, Lightspeed relies on the enclosed Standard Contractual Clauses (“SCCs”), attached hereto as Schedule 2, as an approved transfer mechanism for international transfers of Personal Data. In these SCCs, Customer is the data exporter and Lightspeed Commerce Inc. is the data importer.

d) Signature of the Service Agreement shall be deemed to constitute signature and acceptance of the SCCs. If Customer would like to additionally execute a separate copy of the SCCs, Customer may complete the appropriate pre-signed version attached hereto as Schedule 2, countersign it, and return it to Lightspeed by email at privacy@lightspeedhq.com, indicating, if applicable, the Customer’s legal entity and/or account number (mentioned on the applicable Lightspeed Order Form or invoice).

e) In the absence of the aforementioned appropriate safeguards, Lightspeed may – to the extent permitted under and in accordance with applicable data protection laws (including GDPR) – rely on a derogation applicable to the specific situation at hand (e.g. the data subjects’ explicit consent, the necessity for the performance of an agreement, the necessity for the establishment, exercise or defense of legal claims).

f) In relation to transfers of personal data protected by the UK Data Protection Act 2018, the SCCs apply and are deemed amended as specified by the UK Addendum, which is deemed executed by the parties and incorporated by reference into this DPA. Any conflict between the terms of the SCCs and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.

11. Data inquiries.

Any Customer may, at any time, contact Lightspeed at privacy@lightspeedhq.com with all questions and suggestions concerning data protection.

For Customers established in Germany only: Customer may contact Lightspeed’s Data Protection Officer:

Karina Filusch

Friedrichstraße 95

D-10117 Berlin

Germany

Email: info@datenschutzbeauftragte-berlin.eu

With a copy to: privacy@lightspeedhq.com

12. General provisions.

a) **Amendments.** Any amendments or supplements to this DPA must be made in writing. The same applies to any waiver of any right or obligation under this DPA. The order of precedence of individual contractual agreements shall remain unaffected thereby. Lightspeed reserves the right to amend this DPA at any time with effect for the future. Amendments will only be made if the following objective reasons exist:

- if the amendment helps to bring the DPA in line with applicable law, in particular if the applicable legal situation changes;

- if the amendment enables Lightspeed to comply with mandatory judicial or administrative decisions
- if the amendment reflects details of a new or updated Lightspeed Service or of new or updated technical or organizational processes and the existing contractual relationship with Customer is not affected to Customer's detriment;
- if the amendment is solely to Customer's advantage.

b) **Severability.** If any provision of this Agreement is or becomes invalid or impracticable in whole or in part, the validity of the remaining provisions shall not be affected thereby.

c) **Term.** This DPA shall be effective for the entire Term (as defined in the Service Agreement) and this DPA terminates on the date on which the Service Agreement has expired or is terminated.

Schedule 1: Description of Lightspeed's Security Measures

Lightspeed has taken appropriate and sufficient technical and organizational security measures to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where processing involves a transmission of Personal Data over a network, and against all other unlawful forms of processing.

Lightspeed has an established information security organization managed by the Lightspeed security team and is led by the Vice-President for Information Security. Lightspeed Security established and maintains policies and procedures to delineate standards for logical access on the Lightspeed production environments. The policies also identify functional responsibilities for the administration of logical access and security. Lightspeed Information Security policies are reviewed and approved on an annual basis by Security Leadership and are used to support Lightspeed in meeting the service commitments made to the Customer.

The following description provides an overview of the technical and organizational security measures implemented. Such measures shall include, but are not limited to the following. For more detailed information on the latest state of art measures, please contact us directly.

Data Protection

Lightspeed will process the Personal Data as a Data processor, only for the purpose of providing the Services in accordance with documented instructions from the Customer (provided that such instructions are commensurate with the functionalities of the Services), and as may be agreed to with Customer.

Lightspeed implements and maintains appropriate technical and organizational measures to protect the Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure.

Lightspeed maintains a risk management framework and reviews it at least quarterly to identify changes to its environment, systems and the threat landscape to identify and manage any risks involved with operations and the processing of the Personal Data.

Lightspeed ensures that its personnel who access the Personal Data are subject to confidentiality obligations that restrict their ability to disclose the Personal Data, and undergo information security awareness training on an annual basis.

Lightspeed employs the concepts of least privilege and need-to-know, allowing only the necessary access for users to accomplish their job function. User accounts are created to have minimal access. Access above these least privileges requires appropriate and separate authorization.

Lightspeed enforces Multi-Factor Authentication on all critical applications and infrastructure.

In-transit: Lightspeed implements HTTPS encryption on all of its login interfaces and on every customer site hosted on the Lightspeed products. Lightspeed's HTTPS implementation uses industry standard algorithms and certificates.

At-rest: Lightspeed implements encryption at rest to protect against data loss.

Access control

1. Preventing Unauthorized Product Access

Outsourced processing: Lightspeed hosts its services on third party Hosting infrastructure in form of data centers and Infrastructure-as-a-Service (IaaS). Additionally, Lightspeed maintains contractual relationships with vendors in order to provide the service in accordance with our DPA. Lightspeed relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: Lightspeed hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls of our infrastructure providers are audited for SOC 2 Type II, ISO 27001 and PCI DSS compliance, among other certifications.

Authentication: Lightspeed implemented a strong authentication mechanism for Lightspeed users accessing its customer products. All Lightspeed users who need to interact with the products via any interface must authenticate using multi-factor authentication in order to access non-public Customer data.

Authorization: Customer data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of Lightspeed's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

2. Preventing Unauthorized Product Use

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: Lightspeed implemented a Web Application Firewall (WAF) solution to protect certain hosted customer websites and other internet-accessible applications specifically identified by Lightspeed. The WAF is designed to detect and prevent attacks against publicly available services.

Vulnerability scanning: Lightspeed regularly scans its code, infrastructure and web services for known vulnerabilities and remediates them in a timely manner. Lightspeed subscribes to news feeds for applicable vendor flaws and proactively monitors vendor's websites and other relevant outlets for new patches.

3. Limitations of Privilege & Authorization Requirements

Product access: A subset of Lightspeed's employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Employees may be granted access by role or upon submitting an approved request. Log-ins to data storage or processing systems are logged.

Database access: Customer data is accessible and manageable only by a limited number of authorized staff. Access to data is restricted through network segmentation of the production, staging, quality assurance and development environments. Direct database query access is restricted, and application access rights are established and enforced.

Incident Management Control

Detection: Lightspeed designed its infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregate log data and alert appropriate employees of malicious, unintended, or anomalous activities. Lightspeed personnel, including security, operations, and support personnel are responsive to known incidents.

Response and tracking: Lightspeed maintains a record of known security incidents that includes descriptions, dates and times of relevant activities, and incident remediation. Suspected and confirmed security incidents are investigated by security, operations or support personnel, and appropriate resolution steps are identified and documented. For any confirmed incidents, Lightspeed will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

Communication: If Lightspeed becomes aware of unlawful access to Customer data stored within its products, Lightspeed will: Notify the affected Customers of the incident; Provide a description of the steps Lightspeed is taking to resolve the incident; Provide status updates to the Customer contact, as it deems necessary or is legally required. Notification of incidents, if any, will be delivered to one or more of the Customer's contacts in a form Lightspeed selects, which may include via email or telephone.

[Schedule 2: Standard Contractual Clauses \(Only for Customers established in the European Economic Area, Switzerland or the United Kingdom\)](#)

[Schedule 3: International Data Transfer Addendum to the EU Commission Standard Contractual Clauses \(Only for Customers established in the United Kingdom\)](#)

Dated November 21, 2023

Central Islip Union Free School District

Lightspeed Commerce Inc.

DocuSigned by:
Andrew Chien

Name: _____

Name: Andrew Chien

Title: _____

Title: Head of Commercial Legal, Global (Interim)