

**BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -**

**SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION**

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).

<p><b>Name of Contractor</b></p>	<p>The Digital SLP, LLC</p> <hr/>
<p><b>PII Declaration</b></p>	<p><b>Does your organization/software collect student personally identifiable information (PII) or staff PII?</b></p> <p>Examples of student PII:</p> <ul style="list-style-type: none"> <li>a. The student’s name;</li> <li>b. The name of the student’s parent or other family members;</li> <li>c. The address of the student or student’s family;</li> <li>d. A personal identifier, such as the student’s social security number, student number, or biometric record;</li> <li>e. Other indirect identifiers, such as the student’s date of birth, place of birth, and Mother’s Maiden Name;</li> </ul> <p>Examples of staff APPR PII:</p> <ul style="list-style-type: none"> <li>a. Teacher ID</li> <li>b. Name</li> <li>c. Birthdate</li> <li>d. Gender</li> <li>e. Race</li> <li>f. Salary</li> </ul> <p><input type="checkbox"/> <b>IF YOUR ORGANIZATION/SOFTWARE DOES NOT COLLECT PII, CHECK THIS BOX AND SKIP TO THE BOTTOM, SIGN AND SUBMIT.</b></p> <p>If you collect the PII information above, please complete the remainder of this form.</p>
<p><b>Description of the purpose(s) for which Contractor will receive/access PII</b></p>	<p>In order to create a Staff (SLP)’s account and membership, a person’s name, email address, phone number and billing address is collected and stored within the site. No one except the individual, and the site administrators, have access to this information.</p>
<p><b>Type of PII that Contractor will receive/access</b></p>	<p>Check all that apply:</p> <p><input type="checkbox"/> Student PII</p> <p><input checked="" type="checkbox"/> APPR PII</p>

<b>Contract Term</b>	Contract Start Date <u>09/01/2023</u> Contract End Date <u>08/31/2024</u>
<b>Subcontractor Written Agreement Requirement</b>	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option)  <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor will utilize subcontractors.
<b>Data Transition and Secure Destruction</b>	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> <li>• 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.</li> <li>• Securely delete and destroy data.</li> </ul>
<b>Challenges to Data Accuracy</b>	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.
<b>Secure Storage and Data Security</b>	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)  <input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party. <input type="checkbox"/> Using Contractor owned and hosted solution <input type="checkbox"/> Other:
<b>Encryption</b>	Data will be encrypted while in motion and at rest.

**CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN**


The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	See security storage and data security above. Maintain FERPA certification.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	We limit employee access to student data to only those employees with a need to such access to fulfill their job responsibilities;
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	We conduct regular employee privacy and data security training and education; and
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	we conduct background checks on our employees that may have access to student data; We protect personal information with technical, contractual, administrative, and physical security safeguards in order to protect against unauthorized access, release or use.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	The Digital SLP LLC will promptly notify any affected parties and comply with all local, state and federal laws should a data breach occur. Measures will be taken to immediately rectify and contain any such breach. Should a student's or client's records be divulged in an unauthorized manner, The Digital SLP LLC will keep the district or agency informed and will document what information was divulged and when the incident occurred, along with any other relevant information pertaining to the disclosure.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon termination of a membership, each SLP/teacher user account is retained on the site so that a user may at any point in the future resume or initiate a new membership, print out invoices, or anything related to their account. Students do not receive accounts and no student data is directly stored.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Upon termination of a membership, each SLP/teacher user account is retained on the site so that a user may at any point in the future resume or initiate a new membership, print out invoices, or anything related to their account. Students do not receive accounts and no student data is directly stored.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	We are in compliance with iKeepSafe' FERPA certification.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1	The database is stored on the LiquidWeb dedicated server along with the files for the website. LiquidWeb provides an Acronis backup service which backs up to the LiquidWeb cloud storage on a daily basis. Additional backup data is stored within Dropbox Business; the database

## Western Suffolk BOCES Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("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, 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); and 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.
5. A complete list of all student data elements collected by NYSED is available at [www.nysed.gov/data-privacy-security/student-data-inventory](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. (i) Complaints should be submitted to: [dpo@wsboces.org](mailto:dpo@wsboces.org). (ii) Complaints may also be submitted to the NYS Education Department at [www.nysed.gov/data-privacy-security/report-improper-disclosure](http://www.nysed.gov/data-privacy-security/report-improper-disclosure), by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to [privacy@nysed.gov](mailto: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.

CONTRACTOR	
[Signature]	
[Printed Name]	Jessica Cassity
[Title]	Owner/ CEO
Date:	05/24/2023

January 13, 2022



PDFfiller Document ID: E0AE-4C48-B48B-0000

# The Digital SLP HIPAA, FERPA and Related Privacy and Security Laws Compliance Plan

REVISED: 08/31/2022

The Digital SLP LLC is committed to the safety and security of members and students and their associated records. We take site security and student confidentiality very seriously. To keep student information protected, we have put the following measures in place:

- Our website is hosted on a HIPAA compliant server with physical and network security.
- No student data is directly collected or stored by The Digital SLP at this time.
- Users may make lists of favorite resources, which are accessible only by the same user that created the list, and the user has the option of giving each list a custom title. It is possible that some users will choose to use a student name or ID number in the title of the list. Due to this possibility, the list names are encrypted when stored in the database.
- Data created by each user will be retained for as long as the account is active or is needed to provide services. If a user account is terminated or deactivated, information associated with the account will be retained for at least three years and may be retained as long as is needed for business and legal purposes. Lists created by the user of a terminated or deactivated account will be deleted after three years.
- Any student records (or client records if the client is seen by private practice SLPs) that The Digital SLP LLC comes into contact with are treated with strict confidentiality measures in accordance with all applicable state and federal laws.

This plan is designed to:

- Establish policies and procedures that are designed to ensure compliance with applicable state and federal laws.
- Outline roles and responsibilities related to the maintenance, provision and structure of the site and align security practices with the NIST Cybersecurity Framework.
- List what kind of data is collected and for what purpose.

REVISED: 08/31/2022

---

## USER DATA

On The Digital SLP website, user data such as member names and credit card information is processed, and members may also make “lists” that could include student names or IDs.

### Privacy

User data is protected by secure passwords and unique user accounts. Our [privacy policy](#) details some general and anonymized information that is collected and used for third-party services like Google Analytics or Facebook marketing directed at people who view sales or blog pages.

Actual user data such as names, email addresses, or any related student records, are never shared with third parties like Google or Facebook. Member names, email addresses and billing addresses are shared with payment processors (either Stripe or PayPal) during billing. No student names or information are shared with third parties.

### Types of Data Collected and Why

In order to create a user’s account and membership, a person’s name, email address, phone number and billing address is collected and stored within the site. No one except the individual, and the site administrators, have access to this information.

Credit card information is processed by our payment processors, either Stripe or PayPal.

Website users may make “lists” within the site, and they are free to give the lists whatever name they choose. Given the free-form nature of list naming, some users will name the lists with the name(s) or ID(s) of their student(s) or client(s). At present, this is the only potential area where a student name or “record” may end up.

As detailed later in this document, for safety, the lists names are kept encrypted within the database.

### What Happens Upon Account Termination

Upon termination of a membership, user accounts are retained on the site so that a user may at any point in the future resume or initiate a new membership, print out invoices, or anything related to their account.

---

## **STUDENT / CLIENT DATA**

### **Personally Identifiable Information**

Members of the website may make lists and give these lists the names or IDs of their students or clients. This personally identifiable information is treated with strict confidentiality by The Digital SLP LLC in accordance with applicable state and federal laws.

### **Rights and Responsibilities**

In the case of a student, any school district's or local educational agency's Parents' Bill of Rights for Data Privacy and Security are included, and any student records or data belong to and are under the control of said district or local educational agency.

The data collected or retained pertaining to student or client records are not viewable or usable by anyone other than the website administrators or assignees for the express purpose of troubleshooting any element related to a website member's account. No student or client data, or the website members' data, is sold to any third party or disclosed for marketing purposes.

### **Safeguards**

No unauthorized persons has access or will be granted access to student or client data.

An authorized person is defined as the membership account holder, or any administrators or assignees of The Digital SLP LLC.

Administrators and assignees of The Digital SLP LLC receive notice of the importance and requirement of strict confidentiality when handling any such records or data before they are granted administrator-level access.

These records and data are safeguarded according to the additional provisions within this document.

Any staging environments that are created for the purpose of development or testing will not include any list information (which could include student names) from the live servers.

---

## TECHNICAL SAFEGUARDS

The Information Access Control policy ensures that inappropriate access is prevented and that access is granted upon the “least access necessary” scenario.

### User Accounts

#### Unique user accounts/IDs and passwords

Any person needing access to the website administration or membership areas must be granted a unique username and password so that each person has their own, verifiable and trackable access.

When accessing the website administration area, the membership area or an account information area, each person must be logged into their own, unique user account.

Sharing of user accounts for any reason by any administrator or by website members is expressly prohibited.

Each non-administrator account is only allowed to access items related to their own account, such as their user account information, subscription information, lists, and related information. Access to any other users’ accounts are prohibited by access controls built into the system.

#### Password Policy & Two Factor Authentication

All accounts for The Digital SLP website are required to be secured with a password.

Two factor authentication is required for all administrator accounts and may not be disabled by anyone with administrator-level access.

#### Administrator Accounts

Administrator access is handled sensitively and only people that are required to have full administrator access in order to administer aspects of the site are granted such access.



On a regular basis, administrator accounts are reviewed to ensure that only the appropriate individuals have access.

At any point that any employee, contractor or other such person that has administrator access is removed from their role at The Digital SLP, their administrator account access is immediately terminated.

## Website Updates & Security

WordPress is a website application maintained by the WordPress organization, and like any computer system or application, it frequently releases new versions that add new features and fix security issues and vulnerabilities within its core code.

It also allows for third-party software to be used, and it calls these items “plugins” and “themes.” This third-party software will also frequently release feature and security updates.

In order to ensure the safety and security of the website, The Digital SLP routinely installs any available updates for WordPress, any plugins and any themes, on a weekly basis (or sooner if there are any critical security issues that require immediate attention).

This frequent updating helps to ensure that the website is not the subject of a hacking attempt due to outdated software.

## Firewall & Server

The Digital SLP website is hosted on a physically secure, HIPAA/HITECH compliant server behind a hardware firewall, hosted by LiquidWeb.

The server is a dedicated server that hosts only The Digital SLP website and does not contain any other LiquidWeb customer data.

All server access is protected by a physical Cisco firewall with only the required ports open for website access.

## Physical Server Security

- Located in a 24/7/365 Staffed Facility
- Closed Circuit TV Security Cameras
- Monitored 24/7/365 by 3rd Party Security Company

- Site Entrance Controlled by Electronic Perimeter Access Card System
- High Security Facilities
- Data Centers Privately Owned and Operated
- Durable, Poured Concrete External Walls
- Disaster Neutral Geographic Locations
- Advanced Fire Prevention Infrastructure with Dry Pipe Preaction, Double Interlock System; NFPA 13 Compliant
- Office Space Separate from Data Center Space
- Advanced Proximity Credentials Required to Access Data Center
- All Employees Receive Full Background Check
- Exterior Entrances Secured by Mantraps with Interlocking Doors
- Access to the Data Center Space Requires Secure Credentials
- SSAE-16 (formerly SAS70) & Safe Harbor Compliant

### Server Power Backup

- Uses Uninterruptible Power Supplies (UPS) to ensure the site is always available
- Multiple N+1 MPS Generators
- Multiple Fuel Contracts Ensure Fuel Availability for Generators
- Multiple N+1 UPS Systems with 30 Minute Minimum Runtime
- Redundant ASCO Closed Transition Bypass Isolation Transfer Switches
- Diverse Paths from Substation

### Network Device Security

- Hardware Cisco Firewall with Full Management
- Network Redundancy Ensures Failover
- Diverse Connectivity Fiber Paths Into Building
- Carrier Neutral

### Sucuri Security

In addition to the physical and network security provided by LiquidWeb, The Digital SLP also uses the third-party Sucuri service to provide another layer of firewall and security protection.

Sucuri scans incoming traffic and will attempt to block malicious attempts to access the site or hack into the site..

Malware scanning and remediation is also performed by Sucuri, ensuring that the site is not infected with malware.

## Encryption

All access to and from The Digital SLP website is secured with HTTPS encryption to prevent unauthorized snooping and to secure user data and passwords.

Passwords are stored within the WordPress database via WordPress's built-in encryption system which uses DES to store an encrypted password hash.

Users of The Digital SLP are also able to save "lists," which are collections of activities and materials available on the website, and the users are able to give these lists unique names. As a matter of course, some users may decide on their own to name these lists with the name(s) or ID(s) of their student(s) or client(s).

List names are stored in the database in an encrypted format using the Defuse PHP Encryption library. The key to decode the stored list is not saved in the database, so if the database is ever compromised or stolen, the list names cannot be decrypted without this key.

The key to decode the lists is kept in a separate location in the file system on the server, separate from the database.

## Backups

The Digital SLP employs regular backups of the site, both via LiquidWeb and via Dropbox.

The LiquidWeb backups are full backups of the files and the database that are taken once daily, and retained for seven days.

In order to provide data redundancy and independence from any one vendor, the site files and database are also backed up daily, automatically to a Dropbox Business account which is HIPAA compliant. The database backup is encrypted and cannot be decrypted or used without knowing the password.

<https://help.dropbox.com/accounts-billing/security/hipaa-hitech-overview>

## Staging & Development Server Environments

It is necessary to use staging and development server environments to test and create new features for the website. The staging environments make use of copies of the live website so

that items can be adequately tested to fix bugs or to ensure that new or added features will work before they are deployed on the live site.

Per policy, no “lists” from the live website will be included in the staging and development environments since these lists could contain student names or PII. When copying the live database to a staging and development server, the table containing this information will be dropped and/or wiped clear of this data before activating the staging and development environment ensuring the security and privacy of this data.

---

## **AUDITING**

On a regular basis the following areas are checked and audited by The Digital SLP. Any items found to be out of compliance with any established procedures are remediated on a priority basis as soon as possible to ensure the continued safety and security of the website and all collected and stored data.

### **Administrator Accounts**

Periodically the list of administrator and/or administrative user accounts pertaining to The Digital SLP website are checked to ensure that the correct number of accounts exist, that there are no stale accounts or accounts that should be removed, and that there are no undocumented/unauthorized accounts.

### **Backups**

Backups are checked periodically to ensure that the backups are operating properly, that the website can be restored in the event of any failures, and that the backups are still secured and encrypted according to the provisions in this document.

### **Malware Scans**

The website is regularly and automatically scanned by the third-party Sucuri service provider for website malware. In addition to these automated scans, period manual scans are also run to provide an added layer of security and to ensure that no malware or unauthorized website access is present.

## **Website Updates**

The Digital SLP makes it a regular practice to install any updates for any software used within the website. On a regular basis the site is reviewed to ensure these updates have been applied and that there are no pieces of software that have become abandoned or have been flagged for any known CVE or security vulnerabilities.

---

## **DATA BREACH POLICY**

The Digital SLP LLC will promptly notify any affected parties and comply with all local, state and federal laws should a data breach occur. Measures will be taken to immediately rectify and contain any such breach.

Should a student's or client's records be divulged in an unauthorized manner, The Digital SLP LLC will keep the district or agency informed and will document what information was divulged and when the incident occurred, along with any other relevant information pertaining to the disclosure.