# Method Learning INFORMATION SECURITY PLAN

## April 2025

Corporate Officer: Bryan Ziegler, Vice President

## OBJECTIVE:

The objective of Method Learning (ML) in the development and implementation of this comprehensive written information security program ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of Education Records as defined in 34 CRF §99.3 ("Education Records"), and the Personally Identifiable Information contained therein as defined in 34 CFR §99.3 ("PII") and the confidential records of our customers' end users, including but not limited to our customers' employees (i.e. teachers and principals) and students, (cumulatively, all 'end users'), and to comply with our obligations under the Family Educational Rights and Privacy Act (FERPA) at 20 USC 1232g and any applicable state laws or regulations (the "regulations"). The WISP sets forth our procedure for evaluating and addressing our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PII of all end users.

## PURPOSE:

The purpose of the WISP is to better: (a) ensure the security and confidentiality of Education Records and PII, (b) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; and (c) protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft, fraud, misuse or invasion of privacy.

## SCOPE

In formulating and implementing the WISP, Method Learning has addressed and incorporated the following protocols:

(a) identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Education Records or PII;

(b) assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Education Records and PII;

(c) evaluated the sufficiency of existing policies, procedures, information systems, and other safeguards in place to control risks; including
greatly limiting the intake of sensitive or PII

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

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

## DATA SECURITY COORDINATOR & BUSINESS UNIT REPRESENTATIVE:

Method Learning has designated a Data Security Coordinator to implement, supervise and maintain the WISP. The Data Security Coordinator (DSC) may be an individual and / or may also be comprised of one or more members of the Corporate IT (CIT) staff and shall work with a designated Business Unit (BU) Representative (BUR) to carry out the following data security responsibilities, and as assigned below.

(a) Implementation of the WISP including all provisions outlined in the Operational Protocol as further defined in this Plan.

Responsibility: CTO

(b) Training of all employees.

Responsibility: CTO

(c) Regular testing of the WISP's safeguards that are pertinent to the Business Unit level;

Responsibility: CTO

(d) Evaluating the ability of any of our third party service providers to implement and maintain appropriate security measures for the Education Records or PII to which ML has permitted said third party to access, and requiring such third party service providers by contract to implement and maintain appropriate security measures.

Responsibility: CTO

(e) Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing Education Records or PII.

Responsibility: CTO

(f) Conducting an annual training session for all ML officers, managers, employees and independent contractors, including any temporary and contract employees who have access to Education Records or PII on the elements of the WISP.

Responsibility: CTO

(g) Tracking of assets assigned to ML employees in accordance with the Corporate Asset Tracking Policy.

Responsibility: CTO

## INTERNAL RISK MITIGATION POLICIES:

To guard against internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Education Records or PII, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

**Method Learning**
**Information Security Policy**

(a) ML will only collect personal information of clients, customers, customer's employees or students (i.e. end-users) where it is necessary to accomplish our legitimate business transactions or to comply with any and all regulations. See ML's Privacy Policy

(b) Access to records containing Education Records or PII shall be limited to those employees whose duties, relevant to their job description, have a legitimate need to access said records, and only for this legitimate job-related purpose.

(c) Written and electronic records containing Education Records or PII shall be securely destroyed or deleted at the earliest opportunity consistent with business needs or legal retention requirements. ML's business records needs and associated retention and secure destruction periods are set at two (2) years.

(d) Transmission of Education Records and PII must be kept to a minimum necessary and protected with appropriate safeguards.

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

(f) Terminated employees must return all records containing Education Records or PII, in any form, in their possession at the time of termination. This includes all data stored on any portable device and any device owned directly by the terminated employee.

(g) A terminated employee's physical and electronic access to records containing Education Records or PII shall be restricted at the time of termination. This shall include remote electronic access to personal records, voicemail, internet, and email access. All keys, keycards, access devices, badges, company IDs, business cards, access to all SaaS subscriptions licensed by ML and the like shall be surrendered at the time of termination.

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

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

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

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

(l) Access to Education Records and PII is restricted to approved and active user accounts.

(m) Current employees' user ID's and passwords shall conform to accepted security standards.

(n) Employees are required to report suspicious or unauthorized use of Education Records or PII to a supervisor, the Data Security Coordinator or his/her designee(s).

(o) Whenever there is an incident that requires notification pursuant to any applicable regulations the Data Security Coordinator or his/her designee(s) shall host a mandatory post-incident review of events and actions taken, if any, in order to determine how to alter security practices to better safeguard Education Records and PII.

**EXTERNAL RISK MITIGATION POLICIES:** All system security software including malicious code protection, internet security including firewall protection, operating system security patches, and applicable software products shall be reasonably up-to-date and installed on any ML computer that stores or processes Education Records or PII.

There shall be secure user authentication protocols in place that:

(a) Control user ID and other identifiers;

(b) Assigns passwords in a manner that conforms to accepted security standards, or applies use of unique identifier technologies;

(c) Control passwords to ensure that password information is secure.

Education Records and PII shall not be removed from the business premises in electronic or written form absent legitimate business need and use of reasonable security measures, as described in this policy.

**OPERATIONAL PROTOCOL:** The Operational Protocol shall be reviewed and modified as deemed necessary at a meeting of the Data Security Coordinator, the corresponding BU Representative and any other personnel responsible for the security of Education Records and PII. The review meeting shall take place during the first quarter of each year. Any modifications to the Operational Protocol shall be published in an updated version of the WISP. At the time of publication, a copy of the WISP shall be distributed to all current ML employees and to new hires on their date of employment.

**1. Recordkeeping Protocol:** ML will only collect personal information of clients and customers and employees that is necessary to accomplish ML's legitimate business transactions or to comply with any and all regulations. (See ML's Privacy Policy)

Any Education Records or PII stored shall be disposed of when no longer needed for business purposes or required by law for storage. Disposal methods must be consistent with those prescribed by the WISP.

Any paper files containing Education Records or PII of clients, employees, students or end-users shall be stored in a locked filing cabinet or room at the end of each day.

All employees are prohibited from keeping unsecured paper files containing Education Records or PII in their work area when they are not present (e.g. lunch breaks).

Paper or electronically stored records containing Education Records or PII shall be disposed of in a manner that complies with any applicable regulations, which may include the following (which services may be provided by a third party specializing in such procedures):

(a) paper documents containing Education Records or PII shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;

(b) electronic media and other non-paper media containing Education Records or PII shall be destroyed or erased so that the Education Record or PII cannot practicably be read or reconstructed.

Electronic records containing Education Records or PII shall not be stored or transported on any portable electronic device, sent or transmitted electronically to any portable device, or sent or transported electronically to any computer, portable or not, without being encrypted. The only exception shall be where there is no reasonable risk of unauthorized access to the Education Record or PII or it is technologically not feasible to encrypt the data as and where transmitted.

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

**2. Access Control Protocol:** All ML computers shall restrict user access to those employees having an authorized and unique log-in ID.

All visitors who are expected to access areas other than common space or are granted access to office space containing Education Records or PII shall be required to sign-in and/or accompanied by an authorized employee.

All visitors are restricted from areas where files containing Education Records or PII are stored. Alternatively, visitors must be escorted or accompanied by an approved employee in any area where files containing Education Records or PII are stored.

All systems with an internet connection or any ML computing device that stores or processes Education Records or PII must have a reasonably up-to-date version of malicious code protection software installed and active at all times.

**3. Third Party Service Provider Protocol:** Any ML service provider or individual that receives, stores, maintains, processes, or otherwise is permitted access to any file containing Education Records or PII ("Third Party Service Provider") shall be required to meet the following standards (where such Third Party Service Providers will include third parties who provide off-site backup storage copies of all ML electronic data; paper record copying or storage service providers; contractors or vendors working with ML's customers and having authorized access to ML records):

(a) Any contract with a Third Party Service Provider who will have access to the Education Records or PII of end-users shall require the Service Provider to implement security standards consistent with the security protocols defined in this WISP.

**BREACH OF DATA SECURITY PROTOCOL:** Should any employee know of a security breach at any of ML's facilities, or that any unencrypted Education Record or PII has been lost or stolen or accessed without authorization, or that encrypted Education Records or PII along with the access code or security key has been acquired by an unauthorized person or for an unauthorized purpose, the following protocol is to be followed.

(a) Employees are to notify the Director of CIT, Business Unit Representative or the employee's manager in the event of a known or suspected security breach or unauthorized use of Education Records or PII. The Data Security Coordinator, Director of CIT, Legal Counsel or Privacy Officer, Business Unit Representative or the employee's manager must then report any such known or suspected breach or unauthorized use to their Executive Vice President who shall also ensure that the Data Security Coordinator, Privacy Officer and Legal Counsel are aware of the suspected breach or unauthorized use.

(b) The Data Security Coordinator or his/her designee(s) shall be responsible for drafting a security breach notification to be provided to the relevant persons, as appropriate. The security breach notification shall include the following:

(1) A detailed description of the nature and circumstances of the security breach or unauthorized acquisition or use of Education Record or PII; (2)

The number of applicable persons affected at the time the notification is submitted;(3) The steps already taken relative to the incident; (4) Any steps intended to be taken relative to the incident subsequent to the filing of the notification; and (5) Information regarding whether law enforcement officials are engaged in investigating the incident.

Addition Security Information Located Here:
https://methodize.methodlearning.com/security

Privacy Policy:
Privacy Policy

General Terms and Conditions:
General Terms and Conditions