Client Data Privacy Compliance Policy

Version number	2.1
Last Approved	Feb 25, 2025
Classification	PUBLIC

Overview

The Client Data Privacy Compliance Policy provides the framework for The Company's requirements for implementing and maintaining privacy compliance across all applicable laws and regulations.

Applicability

The applicability of this statement falls under purview of the Security Documentation Overview .

Scope

The Client Data Privacy Compliance Policy defines the key components of handling client data and SaaS-related data with consideration of The Company's privacy capabilities and obligations.

Client Data Privacy Compliance Policy

Privacy Governance

Client Data Privacy Oversight

The Company's Head of Legal has overall accountability for The Company's compliance and oversees the execution of all related policies and procedures.

The Company's VP Information Security is responsible for ensuring that all requirements are defined in policy and that processes and controls are in place and are measured for effectiveness.

Public Privacy Notice

The Company publishes a publicly-facing Privacy Notice - Learning Technologies Group that discloses how The Company captures, stores, and processes personal data.

Independent Privacy Compliance Validation

The Company has a defined audit process to ensure ongoing compliance and effectiveness of procedures and controls related to client data privacy. This process includes internal and external audits and certifications, including:

- EU-US Data Privacy Framework program (EU-US DPF) and the UK Extension to EU-US DPF (UK-US DPF)
- SOC 2 Type 2
- ISO 27001
- ISO 27701

Technical and Organizational Measures

The Company implements and maintains reasonable and appropriate technical and organizational measures for the security, confidentiality, and integrity of client personal data aligned with:

- the risk and nature of the personal data
- Industry standard and norms
- the costs of implementation
- the nature, scope, context, and purposes of processing

These measures include, but are not limited to:

- Information Security Statement
- Business Continuity Planning and Disaster Recovery Policy
- Data Classification and Handling Policy
- Data Encryption Policy
- Data Retention, Destruction and Disposal Policy
- Vulnerability Management Policy
- Physical Security Policy
- Vendor Management Policy
- Security Incident Response Plan
- Secure Software Development (SDLC) Policy
- Security Awareness Training

- Change Management Policy

Product Development

The Company practices secure software development ***privacy by design*** to ensure that systems support privacy requirements by default.

Aspects of this approach include, but are not limited to:

- Data minimization
- Audit logs
- Privacy requirements are built into the Secure Software Development (SDLC) Policy
- Consent management

Participating Parties

Company Personnel

Confidentiality and integrity requirements are incorporated the employment agreements of all Company Personnel.

- All Personnel are also required to undergo privacy training as a part of their onboarding process and have passed a background check, where lawful.
- Personnel must pass an annual training that covers both security and privacy.

3rd Party Management

All Sub-Processors of data belonging to The Company's clients must undergo initial and thereafter annual risk assessment. The Company's Vendor Risk Assessment process is detailed in the Vendor Management policy.

The key principle driving sub-processor risk assessment is ensuring that The Company's privacy commitments to its clients are cascaded to its sub-processors contractually and in practice. Sub-processors are required to have a DPA in place, with exceptions documented.

Client Roles & Responsibilities

In the context of The Company's products, the client is always the Data Controller and The Company is the Data Processor.

As the Data Controllers, clients must determine what data they store and process, and are responsible for determining what privacy obligations are applicable and ensuring The Company is meeting those obligations.

Authorized forms of client data manipulation are established as part of the client's initial contractual agreement.

As part of normal operations within Company services, client administrators routinely make changes to their own data. When those administrative duties are outsourced to The Company (as a contracted service), Personnel assigned to administer client data are authorized (by contractual agreement) to make appropriate changes within the scope of services rendered.

Any approved support requests are acceptable forms of authorization, provided they come a standard support channel, used to assign work tasks to individuals or groups (as requested by clients, designated data owners, or Company management in support of troubleshooting efforts or customer submitted change requests).

Data Subjects

The Company will notify the Client of any data subject request received directly. The Company will comply with contractual, legal, and regulatory requirements with regards to assisting the Client in fulfilling data subject requests to the extent reasonable.

Additional Information

Additional information related to *Disciplinary Actions*, *Exceptions* and *Questions* can be found in the Security Documentation Overview .

Document control

This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	@Art Machado	
Author(s)	@Art Machado @PaulGordon @angelakilmer	
Required Approver(s) and Approval Date	@Art Machado - VP Information Security	Feb 25, 2025
Review cycle	ANNUAL	
Next review date	Feb 24, 2026	

Version History

Date	Author(s)	Version	Changes
Aug 19, 2025	@angelina.kilmer	2.1	Updated Data Subject section
Feb 25, 2025	@Art Machado @angelina.kilmer @Paul Gordon	2.0	Annual review
Nov 1, 2024	@angelina.kilmer	1.12	Changed Policy classification from Confidential to Public
Mar 22, 2024	@Sarah Zwicker (Unlicensed) @Paul Gordon	1.11	Added additional client responsibilities
Mar 12, 2024	@Art Machado , @Sarah Zwicker (Unlicensed) , @Paul Gordon	1.10	Annual review, update links
Aug 17, 2023	@John Cole & @Sarah Zwicker (Unlicensed)	1.9	Policy title change, reorganization, additional cross references and updated TOMs
Feb 23, 2023	@Sarah Zwicker (Unlicensed) & @Art Machado	1.8	Annual review + logo update

Mar 24, 2022	@Sarah Zwicker (Unlicensed)	1.7	Added Privacy considerations and components; linked ISMS-0021
Mar 16, 2022	@Sarah Zwicker (Unlicensed) & @Art Machado	1.6	Title change for VP InfoSec, Annual Review
Jul 27, 2021	@Art Machado	1.5	Added “privacy by design” considerations
Mar 12, 2021	@Sarah Zwicker (Unlicensed)	1.4	Changed owner, updated Overview
Feb 9, 2021	@Sarah Zwicker (Unlicensed)	1.3	Reformatted, policies linked
Jan 26, 2021	@John Cole	1.2	Annual review
Nov 23, 2020	@Sarah Zwicker (Unlicensed)	1.1	Ownership change