



Privacy Policy v4.6

The privacy of our clients' data is paramount to our Clients and to Us. In the course of providing services, we receive, store and manage data that may contain personally identifiable information that may be restricted from disclosure under one or more provisions such as FERPA (US Family Educational Rights and Privacy Act), or HIPAA (US Health Insurance Portability and Accountability Act) or rules such as COPPA (US FTC's Child Online Privacy Protection Act). Longsight implements privacy by design (private, institutional repositories) as well as privacy by default (all options are set to private unless explicitly set otherwise). We treat ALL information from our clients as confidential. We protect client information with the same measures we use to protect our own information. We do not share any client information with anyone without express written permission from you.

1. Privacy compliance

- 1.1. Your data are considered to be confidential and will not be shared beyond Longsight without your express written permission, as regulated by law.
- 1.2. We agree to comply with all state and federal privacy and security legislation as required by law.
- 1.3. The Confidentiality Agreement of the Longsight Employee Handbook requires all Longsight employees to protect Your Confidential Information and Your Covered Content from all unauthorized exposure as part of Our terms of employment. Longsight Employees must immediately report any observed, attempted or suspected security incidents to a Longsight manager including theft, loss or misplacement of media, computing equipment or devices, unauthorized access or disclosure of information, or notification of malware on a Longsight owned and/or managed system.
- 1.4. We will report, either orally or in writing, to You any use or disclosure of Your Confidential Information or Your Covered Content not authorized by this Agreement or in writing by You, including any reasonable belief that an unauthorized individual has accessed Your Confidential Information or Your Covered Content. We will make the report to You immediately upon discovery of the unauthorized disclosure, but in no event more than one (1) business day after We reasonably believe there has been such unauthorized use or disclosure.
- 1.5. Our report shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the Confidential Information or Covered Content used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what We have done or will do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action We have taken or will take to

prevent future similar unauthorized use or disclosure. We will provide such other information, including a written report, as reasonably requested by You.

- 1.6. In the course of providing services during the term of this Agreement, Longsight may have access to student education records that are subject to the US Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, et seq., to personal information that is subject to protections under the US Health Insurance Portability and Accountability Act (HIPAA), or to personal information that falls under the guidelines of the US Child Online Privacy Protection Act (COPPA). All such information is considered confidential and is therefore protected. To the extent that Longsight has access to personal information under this Agreement, we are deemed a “school official,” as defined under FERPA, or as an “operator” under COPPA (FAQs Section M1-M5). We shall not use such personal information for any purpose other than in the performance of this Agreement. Except as required by law, we will not disclose or share personal information with any third party unless permitted by the terms of the Agreement or to subcontractors who have agreed to maintain the confidentiality of the personal information to the same extent required of Us under this Agreement.
- 1.7. In the event any person(s) seek to access Your Confidential Information or Your Covered Content, whether in accordance with FERPA, HIPAA, COPPA or other State, Federal, or relevant international law or regulations, we will inform You immediately of such request in writing if allowed by law or judicial and/or administrative order. We will not provide direct access to such data or information or respond to individual requests. We will only retrieve such data or information upon receipt of, and in accordance with, written directions by You and shall only provide such data and information to You. It shall be Your sole responsibility to respond to requests for data or information received by Us regarding Your data or information. Should We receive a court order or lawfully issued subpoena seeking the release of such data or information, We will provide immediate notification to You of receipt of such court order or lawfully issued subpoena and will immediately provide You with a copy of such court order or lawfully issued subpoena prior to releasing the requested data or information, if allowed by law or judicial and/or administrative order.
- 1.8. If we experience a security breach concerning any of Your Confidential Information or Your Covered Content, then we will notify You within 24 hours of discovery of the breach and take immediate steps to limit and mitigate such security breach to the extent possible. We agree to indemnify and hold you harmless for any loss, cost, damage or expense suffered by you, including but not limited to the cost of notification of affected persons, as a direct result of the unauthorized disclosure of education records.

2. Online engagement

- 2.1. Our websites may use cookies for a variety of purposes. These cookies may provide us with information, including personal information, other information about devices and networks You utilize to access our websites and information

regarding Your interactions with and in our websites. We will treat all such collected information as Your Confidential Information.

- 2.2. Web beacons, tags and scripts may be used in our websites or in emails. These assist Us in delivering cookies, counting visits to our websites, understanding usage and campaign effectiveness and determining whether an email has been opened and acted upon. We may receive reports based on the use of these technologies by our service providers on an individual and aggregated basis.
- 2.3. We own and operate several online platforms, including but not limited to websites in the longsight.com domain, Facebook.com and Twitter.com. By tagging @, #, or other sponsored terms or by commenting, liking, posting or otherwise engaging with the Longsight brand, You grant a nonexclusive, royalty-free, perpetual, transferable, irrevocable and fully sub-licensable right to use, reproduce, modify, distribute, publish, create derivative works from and publicly display such content that You post in any media, now known or hereafter devised, for any purpose. You also permit to use the name that You submit in connection with such content. The connecting content will be treated as non-confidential and non-proprietary. We take no responsibility for any content submitted by other users that uses the aforementioned terms or is otherwise submitted to and is not liable for said content.

3. Data storage and retention

- 3.1. Daily backups of systems, files and data will be done on a cyclical basis, so that any restoration of the system will not result in more than 24 hours of data loss provided We are notified immediately. Longsight shall retain backup sets remotely for thirty (30) days after creation.
- 3.2. Longsight shall maintain a separate Disaster Recovery Plan and share the appropriate elements of the Plan with You at Your request.
- 3.3. Longsight's data retention policy is part of our terms of service and ensures that We will securely transfer to You or You may securely retrieve a complete copy of Your Covered Content as long as you have paid all subscription fees, and that We will completely expunge Your Covered Content from all Longsight Service servers within sixty (60) days after the Termination Date.

4. Insurance

- 4.1. We will present evidence of \$2 million or more in liability insurance including cyber risk insurance.

5. Changes to the policy

- 5.1.1. This policy may be updated from time to time. Updates will become effective as soon as they are published at www.longsight.com If there are any material changes to these policies, You will be notified by email prior to the change being published and becoming effective. Your continued use of Longsight Services or websites constitutes your agreement to be bound by

such changes to the policy. Your only remedy, if you do not accept the updated terms of a Longsight policy, is to discontinue use of the Longsight Services.

6. Definitions

- 6.1. Confidential Information: means the information that you have provided to us as part of the contracting or purchasing process. By example, this would include names, addresses, email addresses, phone numbers, account numbers, purchase orders, and other information that is not included in Your Covered Content. Confidential Information would also include the terms and pricing of the Longsight Service under this Agreement, Your Covered Content and all information clearly identified as confidential at the time of its disclosure.
- 6.2. Your Covered Content: means all Longsight service data that You, Your agents or your end users provide to us as part of the use of Longsight's Sakai services. By example, this may include, among other data, the student name or identifier, student email address, student submissions, course names, grades, comments and annotations that may be associated with a student or instructor.
- 6.3. Us, We, Our and related terms means the company named Longsight, Inc. who developed and hosts the services, as represented by Longsight Employees.
- 6.4. Longsight Employees are US citizens serving as full-time, salaried employees of Longsight, Inc. for whom a background check has been completed, and who have signed the Longsight Employees' Handbook which requires adherence to security practices and includes a strict confidentiality agreement.
- 6.5. You, Your and related terms means the subscribing entity and all affiliated personnel who use the Longsight Sakai service. By example, You would mean the college, school district, university or company whose agents and end users access Longsight Sakai services.
- 6.6. Client means any organization or individual with whom Longsight has an active agreement for services.

Questions about this Privacy Policy should be directed to information@longsight.com