Lightspeed Systems

Protecting Privacy

Lightspeed Systems Overview

prepared by Lightspeed Systems

September 2014

Lightspeed Systems
106 East Sixth Street Suite 500 | Austin, TX 78701
Toll-free: 877. 447.6244
Local: 661.716.7600
lightspeedsystems.com

Lightspeed Systems

Contents

Lightspeed Systems Commitment to Protecting Privacy

Our solutions connect technology and teaching in ways that make collection and use of data necessary. Lightspeed Systems is committed to the privacy and security of its customers. We focus on security fundamentals, including secure practices to ensure that data shared and collected remains private and protected.

1. We will always be transparent in the data we collect and how it is used
2. We will only collect the data that is necessary for the solutions and functions the school has purchased/contracted
3. We will always treat that data with utmost security and privacy
4. We will never sell that data; we will never share it without authorization from the customer; and we will never use it to attempt to sell advertising to students

Data Collection

It is Lightspeed Systems policy to limit the collection of personal information from children and staff to only that which is necessary to utilize Lightspeed Systems products and services.

What data does Lightspeed Systems collect?

For all Lightspeed Systems products and services (e.g., My Big Campus), we may collect the following types of personally identifiable information directly from children: first name; last name; email address; mobile phone number and carrier (optional for notifications); password; IP address; grade level; and school. We may also generate a login ID for the child that is different than the child's actual name.
Non-Personally Identifiable Information: We may collect certain non-personally identifiable information from visitors to our site, such as the date and time of their visit, the type of browser used (e.g., Chrome, Firefox, Internet Explorer), the type of operating system used (e.g., Windows 7 or Mac OS), the ISP from which the visitor receives Internet access, and aggregate information regarding what pages users of the site access or visit.
We may also collect non-personally identifiable information from registered members and match it to personally identifiable information (such as the member's name) in our database. Such combined information is kept in our internal database under the member's user name.

Lightspeed Systems gathers information about all users collectively, such as what areas users visit most frequently and what services users access most often. Lightspeed Systems automatically logs IP addresses, session sources, and other data which tracks users' access to the Services. We analyze these logs for sales and marketing purposes as well as system performance monitoring. These logs are analyzed for the aggregate trends they reveal

about our customers and how the customers use the Services, not for the behaviors of individual users.

Our complete current Lightspeed Systems privacy policies can be viewed here:
http://www.lightspeedsystems.com/privacy/

How does Lightspeed Systems use cookies to collect data?

Lightspeed Systems use cookies to store a customer's session while using My Big Campus. The cookie notifies My Big Campus when a customer has returned to the website without storing the customers' information or password.

Does Lightspeed Systems use a student information system?

Lightspeed Systems has partnered with Clever to help protect student information. Clever is well-trusted instant login software that allows schools to safely connect to the learning applications students and teachers use. Clever links information from a school's SIS and does not access any student data.
Clever's security overview can be viewed here:
http://assets.clever.com/documents/clever-security.pdf

Network Operations Center Management and Security

Does Lightspeed Systems perform tests to identify vulnerabilities within their network?

Yes, Lightspeed Systems performs vulnerability management and intrusion prevention testing. Vulnerability management allows us to identify, classify, remediate, or mitigate vulnerabilities.

Are all network devices located in secure facilities and under controlled circumstances?

Yes, network devices are protected in multiple data centers by a variety of different security measures. Lightspeed Systems uses a combination of restricted access, identification cards, access logs, biometric scanners and two-factor authentication for hosted services.

Are backups performed and tested regularly and stored off-site?

Yes, backups are performed regularly and range from realtime to once daily replication. Data is stored at geographically different locations to further secure the information being stored. Our master databases have fully redundant replicas spread out across multiple data centers in multiple locations.

How are these backups secured? Disposed of?

Lightspeed Systems uses on-line storage secured in data centers to house our backups. Only authorized persons with specific identification credentials can gain access. The entire data center interior and exterior is monitored by cameras and regular manned security patrols.

Disposal of backups is handled in accordance with Life Cycle rules and range from 15 days to 1 year to delete backups.

Are software vulnerabilities patched routinely or automatically on all servers?

Yes, we subscribe to services and monitor security bulletins to determine risks and threats to our systems. System updates are routinely performed to address all security risks that apply to our systems.

Data Storage and Data Access

Where will the information be stored and how is data "at rest" protected?

All information is stored in highly secured datacenters. Data such as passwords are encryted with a cryptographic hash function.

How will the information be stored?

Data is stored in the Cloud with multi-tenant hosting and secured in our remote datacenters. Lightspeed Systems also complies with the Family Education Rights and Privacy Act (FERPA), which requires that school records be maintained separately, and not be mingled with data from other school systems or users.

Details on Lightspeed Systems compliance with FERPA can be viewed here: http://www.lightspeedsystems.com/wp-content/uploads/2012/12/FERPA-Compliance.pdf

In addition Lightspeed System is in alignment with guidelines from Privacy Technical Assistance Center, U.S. Department of Education (PTAC), which provides relevant information and guidance on privacy, confidentiality, and security resources for student data systems.

Where are the servers physically located?

Lightspeed Systems uses secure datacenters to house our servers. Access to physical servers requires keying in an access code and providing a matching physical hand scan. Also only authorized persons with specific identification credentials will gain access. Once the authorized persons have been verified the data center interior requires further credentials to continue. The entire data center interior and exterior is monitored by cameras and regular manned security patrols. Upon exiting the facility, authorized personnel must check out with the security desk and have any bags or boxes inspected. If personnel remove equipment from the data center, they must provide a description of the equipment along with a serial number if possible. This information is logged and a signature on that log entry is required.

How does Lightspeed Systems protect data in transit?

Sensitive data is hashed and sent through Secure Sockets Layer (SSL).

Who has access to information stored or processed by Lightspeed Systems?

Support and Development staffs have access to data processed by Lightspeed Systems. All employees that provide direct support with students and school staff undergo background checks upon hire.

Additionally customers are required to be on a Support Entitled User (SEU) list for their organization in order to gain support on their account. Calls from persons not on the SEU list are verified with district personal and added to the list before providing support.

All customer questions regarding our privacy policy and Safe Harbor compliance should be directed to our Privacy Officer John Genter at privacy@lightspeedsystems.com.

If student or other sensitive data is transferred/uploaded to the provider, are all uploads via SFTP or HTTPS?

Lightspeed Systems has partnered with Clever to help protect student information. Clever requires that all data transfer via its website use the Transport Layer Security (TLS) or Secure Sockets Layer version 3 (SSLv3) cryptographic protocol over a HTTPS connection. This means that unique session keys are used to encrypt and decrypt data transmissions and to validate transmission integrity.

Data and Metadata Retention

How does Lightspeed Systems ensure the proper management of data?

Lightspeed Systems staff members who have access to any student data are required to pass an exam on Lightspeed Systems privacy policies, acceptable use of data, and Safe Harbor as well as agree to strictly follow all privacy, security, and data policies.

How will the Lightspeed Systems delete data?

Customer information and deletion of user accounts can be provided upon customer's request.

Development and Change Management Process

Does Lightspeed Systems follow standardized and documented procedures for coding, configuration management for all servers involved in delivery of contracted services?

Yes, Lightspeed Systems has internal documents and procedures for coding and deploying the applications.

Lightspeed Systems utilizes an adapted version of SCRUM (http://en.wikipedia.org/wiki/Scrum_(software_development)) development practices to develop software. For programing standards and syntax we have adopted the Github Style guide (https://github.com/styleguide). Team code reviews help ensure adherence to standards and proper documentation. Lightspeed Systems products range from hosted to on-premise solutions. To address the specific needs of each product we have developed systems and tools to ensure consistent development, testing, and deployment of software.

Does Lightspeed Systems notify the School System about any changes that will affect the security, storage, usage, or disposal of any information received or collected directly from the school?

Yes, Lightspeed Systems will notify customers via the Community Site and/or email of changes that impact their data such as retention time frames, disposal time frames, changes to data usage, and security measures that change the way customers interact with Lightspeed Systems products.

Availability

Does Lightspeed Systems offer guaranteed service level?

Lightspeed Systems services are available at least 99.5% of the time. Our servers are redundant and continuously monitored for performance and availability. Current performance statistics can be viewed here: http://www.lightspeedsystems.com/sla/

What is the backup-and-restore process in case of a disaster?

Backups are performed regularly and range from realtime to once daily replication. Data is stored at geographically different locations to further secure the information being stored. This includes both physical hardware located in our datacenters or leased rack space and virtual application stacks housed in cloud services. In the event of a system failure, all hosted products can be restored by Lightspeed Systems staff to full operation.

What is Lightspeed Systems protection against denial-of-service attack?

Lightspeed Systems utilizes third-party services to provide 24/7/365 inspection of traffic and DDoS mitigation.

Audits and Standards

Does Lightspeed Systems provide the School System the ability to audit the security and privacy of records?

Lightspeed Systems will work with customers who wish to review the security and privacy of data. This information will require a Non-Disclosure Agreement (NDA) to be in place prior to the review. Customers will only be allowed to review data specific to their organization.

Does Lightspeed Systems comply with a security standard such as the International Organization for Standardization (ISO) or the Payment Card Industry Data Security Standards (PCI DSS)?

Lightspeed Systems partners with data centers that are SSAE16 SOC-1 Type II Certified to store data safely and securely. Cloud compliance is designed and managed in alignment with regulations, standards, and best-practices including, but not limited to: Health Insurance Portability and Accountability Act (HIPAA), Children's Online Privacy Protection Act (COPPA), Family Educational Rights and Privacy Act (FERPA), Privacy Technical Assistance Center, U.S. Department of Education (PTAC), and Federal Information Security Management Act (FISMA). Customer security is further protected with a flexible hybrid cloud platform that provides tools that are tailored to educations specific needs.

Test and Development Environments

Will "live" student data be used in non-production environment?

Lightspeed Systems uses some live data in our non-production testing to ensure that the product performs as expected and for comparative performance testing. These systems require the same access to data as production systems and offer the same high level of security and data protection and privacy. The only difference is a larger number of employees have access to our test environments. All employees who have access to student data whether in production or test environments are required to participate in our PII training and certify they will follow our policies and practices.

Data Breach, Incident Investigation and Response

What happens if your online service provider has a data breach?

Lightspeed Systems will first work to rectify the situation and mitigate further data breach. Once this has been accomplished a thorough Root Cause Analysis (RCA) will be performed and the proper steps taken to ensure the issue cannot occur again. Customers whose data may have been involved will be notified of the incident including details of the data accessed, RCA, and current status of the school's data.

Do you have the ability to perform security incident investigations or e-discovery?

Lightspeed Systems will work with schools to make logs specific to the school's data available. In the event of a security incident, we will endeavor to share critical details as they relate to the school data. This information will require a Non-Disclosure Agreement to be in place prior to the dissemination of the data.

Contact Lightspeed Systems

Lightspeed System policies and procedures are, and will always be, committed to protecting privacy and data while complying with all regulations.
Because Lightspeed Systems products change we are vigilant in reviewing our practices to ensure data remains private. We go to great ends to protect students and to treat their data with care.
Lightspeed Systems takes all concerns about privacy and use of data very seriously.
We believe the organizations that use our products should fully understand the terms and conditions surrounding the use of the information we collect. If you have any questions about this privacy overview, the information that we collect from you, or the Services, please contact our Privacy Officer John Genter at privacy@lightspeedsystems.com.