LIBERTY CENTRAL SCHOOL DISTRICT

District Office, 115 Buckley St. Liberty, NY 12754
845-292-5400 x 2332

Stacy Feasel
District Data Coordinator
Privacy Officer
Community School Coordinator

Data Processing Addendum

This Data Processing Addendum Addendum ("***Addendum***") is entered into by the Liberty Central School District (the "***District***") and TicketSource ("***Contractor***") as of 9/19/2024 (the "***Effective Date***").

WHEREAS, the District is committed to protecting the security and privacy of personally identifiable information ("***PII***") in accordance with all applicable state and federal laws, including but not limited to the Family Educational Rights and Privacy Act ("***FERPA***") and New York State Education Law § 2-d; and

WHEREAS, Contractor has entered into an agreement (the "***Underlying Agreement***" with the District pursuant to which the Contractor may receive PII, including PII of students, teachers and/or principals;

NOW, THEREFORE, the Parties agree as follows:

1. Definitions. All capitalized terms not otherwise defined herein shall have the same definition as used in New York State Education Law § 2-d and/or 8 NYCRR Part 121.

2. Parents Bill of Rights. The District's Parents' Bill of Rights for Data Privacy and Security ("***Parents Bill of Rights***") is attached as Exhibit A and shall be deemed to be expressly appended to and included with the Underlying Agreement.

3. Contractor Responsibilities:
    a. Contractor agrees that PII, including Student Data and Teacher or Principal Data, shall be maintained confidentially and in accordance with federal and state law and the District's data security and privacy policies.

    b. Contractor may not sell, use or disclose PII for any marketing or commercial purpose or permit another person to do so.

    c. Supplemental information concerning Contractor's handling of Student Data and/or Teacher or Principal Data is set forth as Exhibit A-1 to the Parents Bill of Rights.

    d. Contractor shall maintain a data security and privacy plan that complies with the District's data security and privacy policies, as well as all legal requirements, including but not limited to the specific requirements set forth in NY Education

Law §2-d, 8 NYCRR Part 121, and the National Institute of Standards and Technology ("***NIST***") Cybersecurity Framework. At a minimum, Contractor shall:

i. limit access to PII to only those employees or subcontractors that need access to perform Contractor's obligations under the Underlying Agreement;

ii. not use PII for any purpose not authorized under the Underlying Agreement;

iii. not disclose PII to any person without the prior written consent of the parent or Eligible Student, except to the extent such disclosure is made:

1. to an authorized subcontractor for a purpose necessary to fulfill the Contractor's obligations under the Underlying Agreement; or

2. as required under applicable law;

iv. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII received pursuant to the Underlying Agreement; and

v. use encryption to protect PII while in motion or at rest.

e. If Contractor uses a third party to perform any of Contractor's obligations under the Underlying Agreement, Contractor shall ensure that the third party complies with all obligations of the Contractor under this Section 3.

f. Contractor will ensure that any officers or employees of Contractor and, as applicable, Contractor's assignees who have access to Student Data or Teacher or Principal Data have received or will receive training on the federal and state law governing confidentiality of such data prior to receiving access.

4. Breach Notification. Unless otherwise expressly required by law, Contractor agrees to:

a. notify the District promptly, but in no event later than twenty-four (24) hours, after discovery of any data breach or other security incident (collectively, a "***Security Incident***") that is reasonably believed to affect the confidentiality, integrity and/or security of PII, including but not limited to the unauthorized access to or disclosure of such PII;

b. provide the District promptly, but in no event later than five (5) business days, after the notice described in Section 4(a) with a report concerning the known or suspected cause of the Security Incident, the information affected, the steps taken by the Contractor to stop and/or mitigate the Security Incident, and any other information reasonably requested by the District or law enforcement authorities to respond to and/or otherwise recover from the Security Incident; and

c. comply with all other applicable breach notification requirements, including but not limited to those in NY Education Law § 2-d(6) and 8 NYCRR § 121.10.

5. Changes in Applicable Law. PII, including Student Data and Teacher or Principal Data, is subject to rapidly changing laws and regulations. Contractor agrees to work in good faith to execute and implement any additional documents, policies and/or procedures reasonably necessary to comply with any change in applicable law or regulation within thirty (30) days of a request by the District.

6. Termination of Underlying Agreement. Notwithstanding any other provision of the Underlying Agreement, the District may terminate the Underlying Agreement without penalty if (a) Contractor fails and/or refuses to comply with its obligations under this Addendum or (b) the parties are unable to reach agreement on an amendment to this Addendum required by changes in applicable law. At the District's written request, whether upon termination or at any other time, Contractor shall return, de-identify and/or delete all PII in its possession, custody or control. Notwithstanding the foregoing, Contractor shall be entitled to retain (a) archive copies required to be retained (i) by law, (ii) as part of Contractor's business record-keeping (such as without limitation for dispute resolution such as to establish or defend against claims) or (iii) for compliance purposes (such as without limitation audit, tax, privacy or other compliance requirements) or (b) back-up or log files that are not accessible in the ordinary course and deleted on a standard schedule (other than ad hoc back-ups that are deleted outside standard retention windows).

7. Interpretation. In the event of a conflict between the terms of this Addendum (including the attached Parents Bill of Rights) and the Underlying Agreement, the terms of this Addendum and the Parents Bill of Rights shall control notwithstanding any language in the Underlying Agreement to the contrary.

8. Counterparts. This Addendum may be executed in counterparts, each of which shall be deemed an original. Each counterpart may be executed and/or exchanged by electronic means.

IN WITNESS WHEREOF, the Parties agree to be bound by the terms of this Addendum as of the Effective Date:

Liberty Central School District:

By: Stacy Feasel

Signature: *Stacy Feasel*

Title: District Privacy Officer

Date: 9/19/24

Contractor (TicketSource):

By: Emma Baudinette

Signature: Emma Baudinette

Title: Chief Operating Officer

Date: 9/20/24

Exhibit A

Liberty Central School District

Parents Bill of Rights for Data Privacy and Security

The Liberty Central School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. The Liberty Central District establishes the following parental bill of rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.
- The district and its schools, and third-party contractors and subcontractors, will not sell student PII or use or disclose it for any marketing or commercial purposes or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;
- Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see 5500-R);
- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;
- A complete list of all student data elements collected by the State Education Department is available for public review at http://nysed.gov/data-privacy-security/student-data-inventory or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234
- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to the District Security and Privacy Officer, at 845-292-5400 by mail to 115 Buckley Street, Liberty NY 12754 or by email to dataprivacy@libertyk12.org. Complaints can also be directed to the New York State Education Department online at http://nysed.gov/data-privacy-security/report-improper-disclosure, by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@nysed.gov or by telephone at 518-474-0937.

- Parents have the right to be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.
- All district and school employees and officers with access to PII will receive annual training on applicable federal and state laws, regulations, district and school policies and safeguards which will be in alignment with industry standards and best practices to protect PII.
- In the event that the district engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting (Complaints should be directed to the District Security and Privacy Officer at 845-292-5400 by mail to 115 Buckley Street, Liberty NY 12754 or by email to tdefrank@libertyk12.org or can access the information on the district's website www.libertyk12.org

Exhibit A-1

Liberty Central School District

Supplemental Information Relating to Underlying Agreement

Pursuant to New York Education Law §2-d(c) and 8 NYCRR § 121.3(c), the following additional information is provided with respect to processing of Student Data and/or Teacher or Principal Data for the Underlying Agreement between the District and Contractor:

(1) The exclusive purposes for which the Student Data or Teacher or Principal Data will be used are to process ticket sales and provide a ticketing management system for events organized by the Liberty Central School District.

(2) Contractor will ensure that the subcontractors, persons or entities that Contractor will share the Student Data or Teacher or Principal Data with, if any, will abide by data protection and security requirements by methods described here: due diligence is undertaken prior to entering into any contracts with subcontractors. Al subcontractors enter into data processing agreements with TicketSource or have standard contractual clauses added to contracts to ensure compliance with UK/EU data protection laws (GDPR) or the UK/US Data Privacy Bridge. Only data required for the specific processing activity are transferred to the subcontractor (all data transferred is encrypted for security).

(3) The Underlying Agreement expires as set forth in the applicable ordering document. Upon expiration of the Underlying Agreement, and upon written request from the District, Student Data, Teacher or Principal Data will be deleted, and a certification of deletion will be provided to the District. As covered under point 6b, TicketSource may retain booking or event data for one year from the booking date to assist with customer or client booking queries or charge disputes. Data is automatically deleted at the conclusion of one year.

(4) A parent, eligible student, teacher or principal may challenge the accuracy of the Student Data or Teacher or Principal Data that is collected by contacting the District's Data Protection Officer.

(5) Student Data or Teacher or Principal Data will be stored **at AWS cloud-based servers located in North America.**

(6) Contractor will use the security protections **described here: please see our Data Security Statement attached in appendix 1 below.**

(7) Data will be protected using encryption while in motion and at rest.

TicketSource Personal Data and IT Security Policy

TicketSource handles Customer's Personal Data daily. Personal Data must have adequate safeguards in place to protect them, to protect their privacy and to ensure compliance with various regulations including GDPR and PCI DSS.

TicketSource commits to respecting the privacy of all its customers and to protecting any Personal Data from outside parties. To this end management are committed to maintaining a secure environment in which to process Personal Data so that we can meet these promises.

Access to the Personal Data

All Access to Personal Data should be controlled and authorised. Any Job functions that require access to cardholder data should be clearly defined.

- Access to Personal Data and Business Data is restricted to employees that have a legitimate need to view such information.
- No other employees should have access to this Personal Data or Business Data unless they have a genuine business need.
- It is strictly prohibited for employees to download Personal Data or Business Data, unless they have a genuine business need.
- As soon as an individual leaves TicketSource employment, all his/her system logons must be revoked.
- employment.
- If Personal Data is shared with a Service Provider (Sub Processor) then a list of such Service Providers will be maintained as detailed in Appendix A.
- TicketSource will ensure a written agreement is in place with all Sub-Processors to ensure their compliance with GDPR and PCI DSS.
- TicketSource will ensure that a there is an established process including proper due diligence is in place before engaging with a Service provider.
- TicketSource will have a process in place to monitor the GDPR and PCI DSS compliance status of the Service provider.

Access Control – Employee User Accounts

- New user accounts may only be set up at the written request of the Operations Manager or Managing Director.
- When requesting a new user set-up, level of access will be stated and will be based on the requirements of their role, utilising a need-to-know basis.

- Remote access to the TicketSource system will only be granted to staff that are required to monitor the site or support system out of hours.
- A record will be held on each employee's HR file, stating what log-in access and to what platforms or software has been granted.
- When an employment contract concludes, the Operations Manager will request that all user log-ins are disabled on the last day of work and no later. This will either be undertaken by the Internal Developer (computer log-in, TicketSource platform, email, live chat, slack) and the Head of Department (shared log-ins to other platforms or software via LastPass).

Physical Security

Access to sensitive information in both hard and soft media format or accessible by viewing the TicketSource system must be physically restricted to prevent unauthorised individuals from obtaining sensitive data.

- TicketSource will ensure that security at its office is maintained to safeguard any data stored on site.
- Visitors must always be escorted by a trusted employee. At no time should a Visitor be able to view Personal Data or Event Organiser data, or event information and the Visitor must never be left unattended.
- Strict control is maintained over the storage and accessibility of media.
- Employees are only permitted to use storage devices for work purposes with the express permission of a Senior Manager. All data must be deleted from the device when no longer required for that specific work activity.
- All computers that access the TicketSource system where Personal Data can be viewed must have a password protected access and password protected screensaver enabled to prevent unauthorised use. Passwords must never be shared and be regularly changed in line with the TicketSource IT policy.
- Backups of business-critical information is to be stored off-site.
- Remote access to the TicketSource site is restricted to key personnel with responsibilities to monitor the site out of hours.

Disposal of Stored Data / Retention Policy

- All Personal Data within the processing side of the TicketSource system will be securely disposed of when no longer required by TicketSource. Personal Data will be stored for one year for business requirements, specifically to resolve charge disputes or personal charge queries.
- An automated process to permanently delete Personal Data will be run in-line with our retention policy stated above.
- Other data and information (physical or electronic) should be disposed of in accordance with the Retention Policy and Information Classification Policy

Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into company practice to maintain a high level of security awareness. The protection of Personal Data demands regular training of all employees and contractors.

- Undertake Security Awareness and Data Protection training as part of the employee induction process.
- Review handling procedures for Personal Data and hold periodic security awareness meetings to incorporate these procedures into day to day company practice.
- Distribute this security policy document to all company employees to read. It is required that all employees confirm that they understand the content of this security policy document by signing an acknowledgement form.
- Each employee will undertake annual security awareness training.
- All Sub-Processors with access to Personal Data are contractually obligated to comply with regulations such as GDPR and PCI DSS (where applicable).
- Company security policies must be reviewed annually and updated as needed.

Security Management / Incident Response Plan

'Security incident' means any incident (accidental, intentional or deliberate) relating to the TicketSource processing systems. The attacker could be a malicious stranger, a competitor, or a disgruntled employee, and their intention might be to steal information or money, or just to damage the company.

TicketSource has an Incident response plan which is tested once annually.

Employees of TicketSource will be expected to report to the Data Security Officer for any security related issues.

Network security

- Stateful Firewall technology must be implemented where the Internet enters the TicketSource network to mitigate known and on-going threats. Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments such as the business network, and open network.
- All inbound network traffic to TicketSource is blocked by default, unless explicitly allowed and the restrictions have to be documented.
- A topology of the firewall environment must be documented and must be updated in accordance to the changes in the network.
- The firewall rules will be reviewed on a six months basis to ensure validity.
- No direct connections from Internet to the Personal Data environment will be permitted. All traffic has to traverse through a firewall.

System and Password Policy

All employees with access to TicketSource systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

- All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.

- Administrator access to web-based management interfaces is encrypted using strong cryptography.

Anti-virus policy

- All machines must be configured to run the latest anti-virus software as approved by TicketSource. This software must be configured to retrieve the latest updates to the antiviral program automatically on a daily basis. The antivirus should have periodic scanning enabled for all the systems.
- All removable media where permitted to be used (for example USB sticks or storage devices) should be scanned for viruses before being used.
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

Patch Management Policy

- All Workstations, servers, software, system components etc. owned by TicketSource must have up-to-date system security patches installed to protect the asset from known vulnerabilities.
- Where ever possible all systems, software must have automatic updates enabled for system patches released from their respective vendors. Security patches have to be installed within one month of release from the respective vendor.
- Any exceptions to this process have to be documented.

Vulnerability Management Policy

- As part of the PCI-DSS Compliance requirements, TicketSource will run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
- Quarterly internal vulnerability scans must be performed by TicketSource by internal staff or a 3rd party vendor and the scan process has to include that rescans will be done until passing results are obtained, or all High vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.
- Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV). Scans conducted after network changes may be performed by TicketSource's internal staff. The scan process should include re-scans until passing results are obtained.

Protect Data - Transfer of Personal Data to a Sub-Processor

- All third-party companies providing critical services to TicketSource must have a contract to with TicketSource which confirms that they:

1. Adhere to the GDPR and PCI DSS security requirements.
2. Acknowledge their responsibility for securing the Personal Data.
3. Acknowledge that the Personal Data must only be used for assisting the completion of a transaction, providing a fraud control service or for uses specifically required by law.
4. Have appropriate provisions for business continuity in the event of a major disruption, disaster or failure.

5. Provide full cooperation and access to conduct a thorough security review after a security intrusion to the ICO or a Payment Card industry representative, or a Payment Card industry approved third party.

Protect Data – Telephone Box Office Transactions

- Box Office Staff are not permitted to read out card details or repeat back to a customer.
- Box Office Staff are not permitted to write down card details in any format or media, except to enter them directly into the TicketSource system.
- Box Office Staff must talk to the card-holder to obtain card authorisation. If the card-holder is not present, the booking cannot proceed.
- If a card is declined, Box Office Staff are only permitted one further attempt to authorise the card. Following the second attempt, a new card must be entered or request that the personal contacts us again in 24 hours.
- No employee is permitted to have a mobile phone on their desk unless the mobile phone is being used for work purposes (e.g. Developers, Marketing Team) and under no circumstances can photos of a computer screen displaying Personal Data be taken.

Appendix A – Sub Processors

Stripe (Payment Gateway) - Ireland
Postmark (e-ticket and reminder email delivery) - USA
Twilio (mobile ticket delivery) - USA
Amazon (Web Server) – UK / USA
Cloudflare (Website security and application firewall) - UK/Europe/USA (dependent on where the customer is based)
Google Analytics (tracking website traffic) – Europe
XCover (formerly known as BookingProtect) - UK and US