

**PARENT BILL OF RIGHTS FOR STUDENT
DATA PRIVACY AND SECURITY
THIRD PARTY CONTRACTOR SUPPLEMENT**

The BC Technologies Company DBA FinalForms (Vendor) has been engaged by the City School District of Albany (Customer) to provide services. In this capacity, the company may collect, process, manage, store or analyze student and/or teacher/principal personally identifiable information (PII).

The Vendor will provide the district with a proprietary Internet-based data management software. This includes, but is not limited to: conversion of Customers approved forms and data into electronic format; web hosting for online forms; data storage; provision of access to stored data; Customer access to electronic communication tools using online email system, manual notifications or automatic notifications; Customer access to features that allow filtering, sorting, printing and emailing data; email and phone Customer support; and on-line and in-person training. FinalForms collects, processes, formats and stores student data, as requested by Customer.

The Vendor will ensure that subcontractors or others that the company shares PII with will abide by data protection and security requirements of district policy, and state and federal law and regulations by limiting the sharing of PII to only the application host, Amazon Web Services (AWS), and reviewing AWS compliance applicable laws. The *Vendor* by entering into an Agreement with the School District acknowledges it has reviewed the relevant District policies on safeguarding PII, including but not limited to, Policy 8635 and Regulation 8635.

PII will be stored at Amazon Web Services.

- All data is stored within the US.
- FinalForms resides on multi-tenant architecture. Each customer's custom application exists on a unique, secure database.
- AWS hosting facilities meet the highest standards of physical security, redundancy, and monitoring.
- All requests and access to data are executed through HTTPS, SFTP, or SSH.
- Data is encrypted at rest, leveraging SHA 256 encryption.
- Within FinalForms, only Executives, Senior Developers, and Senior Support Staff have access to student data. All FinalForms personnel complete a rigorous, industry standard, background check prior to gaining access to any portion of the FinalForms application.
- FinalForms does not subcontract with any third parties outside of our hosting provider, AWS.

- FinalForms holds personal information, including email addresses as confidential. Unauthenticated inquiries from students, parents, or staff are immediately denied.
- Authorized Parents/Guardians may, at any time, inspect, review, update, or correct form data which they believe to be inaccurate or obsolete. Authorized Administrators may access time-stamped form data change logs based on Parent/Guardian updates at any time for any purpose deemed necessary by the educational institution in accordance with applicable law.

Parents may challenge the accuracy of PII held by *(insert name of contractor)* by contacting *(insert contact information, including title, phone number, mailing address and email address)* the City School District of Albany.

The Vendor will take reasonable measures to ensure the confidentiality of PII by implementing the following:

Physical Security

We host the entirety of our infrastructure on Amazon Web Services (AWS) EC2 and S3 instances. We chose AWS specifically because of its prolific scale, redundancy, and emphasis on data privacy & security. Among its long list of physical security benefits the highlights are:

- Amazon has unmatched experience in designing, constructing, and operating large-scale data centers.
- AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection.
- Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means.
- Authorized staff must pass two-factor authentication no fewer than three times to access data center floors.
- All visitors and contractors are required to present identification and are signed in and always escorted by authorized staff.
- Worldwide facilities have been audited and have received [many certifications](#).
- Linked is the [AWS SOC 3 Report](#).

We have several policies of our own in place that ensure the highest levels of security when handling client information outside of our web application.

- Developer machines do not store sensitive information locally.
- Client information is never stored physically without consent from a client administrator.

Technical Security

Amazon Web Services (AWS) is widely considered to be the leader for infrastructure as a service (IaaS) providers. They [comply with a wide range of regulations](#) and provide granular control over your network. Here are just a few of the many security benefits they provide:

- Host Operating System Security:
 - AWS employees with a business need are required to use their individual cryptographically b SSH keys to gain access to the host.
 - All access is logged and routinely audited.
 - When an AWS employee no longer has a business need to administer EC2 hosts, their privileges on and access to the hosts are revoked.
- Guest Operating System Security:
 - We have complete control over our virtual instances.
 - AWS administrators do not have access to our instances, and cannot log into the guest OS.
- Firewall:
 - Amazon provides a complete firewall solution.
 - This mandatory inbound firewall is configured in a default deny mode and the we must explicitly open any ports to allow inbound traffic.
- Denial Of Service (DoS) Security:
 - Standard DDoS mitigation techniques such as SYN floods and connection limiting are in use.
 - Amazon maintains internal bandwidth which exceeds its provider-supplied Internet bandwidth.
- Man In the Middle (MITM) Security:
 - All of the AWS APIs are available via SSL-protected endpoints which provides server authentication.
- Spoofing Security:
 - The Amazon-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.

- Port Scanning Security:
 - Port scans of Amazon EC2 instances are generally ineffective because, by default, all inbound ports on Amazon EC2 instances are closed.

Outside of the AWS provided features, we implemented and ensure:

- Separate databases are created for each client.
- All administrative activity involving our servers is performed over an encrypted connection.
- Client information is not stored digitally outside of the secure AWS infrastructure.
- Verbose logging is enabled wherever possible, leaving clear audit trails.
- Backups are run periodically and regularly tested for success in recovery situations.
- Intrusion detection systems alert administrators of suspicious activity.

Administrative Privacy

The FinalForms workforce, itself, has been structured to minimize contact with student data. FinalForms requires comprehensive, industry standard, background checks on all employees and/or contractors regardless of their respective role within the business. Data is only ever accessed without school staff present in secure development settings via SSH or through the FinalForms administrative interface, both encrypted connections.

It is ultimately the responsibility of the School District to authorize users with appropriate access.

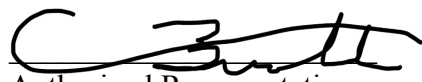
- An Authorized User may supply data to FinalForms, as required by his/her School District.
- Authorized Users using the service provided by FinalForms are responsible for ensuring that they meet the qualifications for the status of Authorized User, as determined by their School District.
- Authorized Users are responsible for ensuring the accuracy and completeness of all information supplied to FinalForms.
- An Authorized User may access and correct personally identifiable information through use of the Service at any time. FinalForms may retain the data supplied by Authorized Users for as long as required by their School District and/or applicable law, or as authorized by the Authorized User.

- An Authorized User is solely responsible for maintaining the confidentiality of his/her user identification and password.
- An Authorized User is solely responsible for all activities that occur in connection with his/her Account.

More information about FinalForms:

- FinalForms does not require an Authorized User to supply it with data.
- FinalForms does not provide or sell any data to third parties.
- FinalForms will not make publicly available the individual data an Authorized User supplies it by using the Service.
- FinalForms will not use any behavioral information to provide targeted advertising to Authorized Users.
- FinalForms will not collect, use, or share behavioral information for any purpose beyond authorized educational or school purposes, or as authorized by the Authorized User.
- FinalForms does not limit a School District's use of the data that an Authorized User supplies FinalForms through use of the Service.
- FinalForms has auditing and logging capabilities which allow internal security analysts to examine detailed activity logs or reports to see who had access, IP address entry, what data was accessed, what data was modified, when it was modified, etc. This usage data may be tracked, logged, stored, and accesses in compliance with applicable law or educational institution policy.
- FERPA does not require particular methods of data destruction. However, other applicable laws or local privacy regulations may require specific secure data disposal methods. Customers should check with their legal counsel to fully understand their data destruction requirements.

The contractor's agreement with the district begins on 7/27/2020 and ends on 7/27/2021. Once the contractor has completed its service to the district, records containing student PII will be returned within 30 days of termination via the following database backup file.


Authorized Representative
(insert name of contractor)

7/27/2020
Date