

Vendor Statement of Compliance Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and
Excel Photographers ("Service Provider") on 06/10/2020 ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

Agree: Yes No

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

Agree: Yes No

3. **PRIVACY.** The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

Agree: Yes No

Section I: General - All Data (Continued)

4. **REUSE:** Vendors shall not copy, duplicate, sell, repack or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.

Agree: Yes No

5. **TRANSPORT:** Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

Agree: Yes No

6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

Agree: Yes No

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?

Agree: Yes No

8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

Agree: Yes No

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

Agree: Yes No

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.
Agree: Yes No
2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.
Agree: Yes No
3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.
Agree: Yes No
4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.
Agree: Yes No
5. Vendor will attach to this document evidence how student data is kept secure and confidential.
Agree: Yes No
6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.
Agree: Yes No
7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).
Agree: Yes No
8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.
Agree: Yes No
9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students
Agree: Yes No

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

Agree: Yes No

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

Agree: Yes No

3. Vendors cannot sell student information.

Agree: Yes No

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

Agree: Yes No

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

Agree: Yes No

6. Vendors must delete district-controlled student information when requested by the District.

Agree: Yes No

7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

Agree: Yes No

As an authorized representative of my organization, I accept the conditions listed in this document.

Malissa Knieriem

Print Name

Malissa Knieriem 6/12/2020

Signature, Date

Laura Assem

Print Name (Roseville City School District)

Laura Assem

Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

Firewalls and active IDS

Section 1.7: Internal Security

Student data is only accessed by management and will be held on secure server

Section II.2: Exporting of Student-Created Content

Exported student data will be used for administrative/school related items such as id cards, yearbook and upload of images to district office for admin software

Section II.4: Review and Correcting Personally Identifiable Information (PII)

Parents or school admin contact us directly via phone or email and we correct errors on our server only

EXHIBITS

Section II.5: Securing Student Data

All student data is kept on secure server with password protected files. Data is only accessed by management

Section II.6: Disclosure Notification

We will notify parents or guardians of security breach by email or phone if necessary

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

We will not disclose any information without written approval of the school site or district office

Section III.5: How Student Data is Protected:

Data is held on secure server and accessed only by management

High5.ID Privacy Policy

Last updated: 2020 10 13. Effective Date: 2020 10 13

High5.ID is a bundle of solutions offered by Excel Photographers located in Sacramento, CA – in this document referred to as “High5.ID”, “us” or “we”. The user of our solutions may be a School, School District, Company, or other group – in this document referred to as “the Organization”, or “you”. People associated with the Organization may include employees, students, visitors – in this document referred to as “Individuals”. A reseller or agent selling or representing our Solution may be a photography studio, independent agent, or other type of relationship – in this document referred to as the “Teammate”.

This privacy policy applies to our High5.ID website and to the High5.ID platform (our “Solutions”) and describes the steps we take to protect your data.

We strive to be transparent in our data collection and use practices. This document describes the personal information we may collect.

1. HOW WE COLLECT AND USE INFORMATION

We collect the following types of information:

- Information about Organizations: We ask for certain information when an Organization representative registers with High5.ID, or if the representative corresponds with us online, including a name and address for the Organization, and a name, email address, and phone number for the contact. We also store an account name, password, and message content. We may also retain information provided by an Organization if the Organization sends us a message, posts content to our website or through our Solutions, or responds to emails or surveys. Once an Organization begins using our Solutions, we will keep records of activities related to the Solutions. We use this information to operate, maintain, and provide to the features and functionality of the Solutions, to analyze our Solutions offerings and functionality, and to communicate with Organizations and Website Visitors.
- Individual Data: High5.ID may have access to personally identifiable information about Individuals (“Individual Data”) in the course of providing its Solutions to an Organization. Examples of such information may include name, photograph, employee or student number, grade, phone number, email address, guardian contact information. We consider Individual Data to be confidential and do not use such data for any purpose other than to provide the Solutions on the Organization’s behalf. Organizations may allow Individuals to log into the Solutions. In that instance, the Organization provides each Individual with login credentials and confirms that it has obtained appropriate parental consent, as needed, before the Individual is permitted to access the Solutions. We receive Individual Data only from the Organization or the Individual’s use of the Solutions.

High5.ID has access to Individual Data only as authorized by the Organization and only for the purposes of performing support to Solutions on the Organization’s behalf. If you are an Individual or the parent of a minor Individual and have questions about the Organization’s use of technology providers like High5.ID, please contact your Organization.

High5.ID does not perform “data mining” activities as it pertains to the analysis and aggregation of Individual Data for the purposes of sharing or selling to third parties. Items or services offered for sale are only offered with the express authorization of your Organization.

We only perform data analysis and aggregation routines to support the use of metrics and reporting capabilities within the Solutions. These results are only visible to authorized Organization users.

We automatically collect certain types of usage information when visitors view our website or use our Solutions. We may send one or more cookies — a small text file containing a string of alphanumeric characters — to your computer that uniquely identifies your browser and lets us help you log in faster and enhance your navigation through the site. A cookie may also convey information to us about how you use the Solutions (e.g., the pages you view, the links you click and other actions you take on the Solutions), and allow us to track your usage of the Solutions over time. We may collect log file information from your browser or mobile device each time you access the Solutions. Log file information may include anonymous information such as your web request, Internet Protocol (“IP”) address, browser type, information about your mobile device, number of clicks and how you interact with links on the Solutions, pages viewed, and other such information. We may track Individual responses to communications including their interactions with SMS, email or other interactive content. This information allows for more accurate reporting and improvement of the Solutions. We may also collect analytics data, or use third-party analytics tools, to help us measure traffic and usage trends for the Solutions. We do not allow third party advertising networks to collect information about the users of our Site or Solutions.

We may use the data collected through cookies, log files, device identifiers, and other tools to: (a) remember information so that a user will not have to re-enter it during subsequent visits; (b) provide custom, personalized content and information; (c) to provide and monitor the effectiveness of our Solutions; (d) monitor aggregate metrics such as total number of visitors, traffic, and usage on our website and our Solutions; (e) provide reporting to Organizations per their requirements, (f) diagnose or fix technology problems; and (g) help users efficiently access information after signing in.

2. HOW WE SHARE YOUR INFORMATION

High5.ID do not rent or sell Individual Data to third parties for marketing purposes. High5.ID will not share or disclose an individual’s confidential information for any purpose unrelated to the safety of that individual via the normal fulfillment of our obligations to client Organizations. Examples of sharing include:

- We may share information with companies that provide us with technology solutions (e.g. SMS broadcasting); this is done strictly for the purpose of carrying out their work for us and only to the minimum required.
- We may be required to share information with law enforcement or other third parties when compelled to do so by court order or other legal process, to comply with statutes or regulations, to enforce our Terms of Use, or if we believe in good faith that the disclosure is necessary to protect the rights, property or personal safety of our users.

If we reorganize or sell all or a portion of our assets, undergo a merger, or are acquired by another entity, we may transfer your information to the successor entity. If we go out of business or enter bankruptcy, your information may not be transferred to a third party.

3. HOW WE STORE AND PROTECT YOUR INFORMATION

Storage and processing: Any information collected through the Solutions is stored and processed in the United States. If you use our Solutions outside of the United States, you consent to have your data transferred to the United States.

Keeping information safe: High5.ID maintains strict administrative, technical and physical procedures to protect information stored on our cloud-hosted servers. Access to information is limited (through

user/password credentials) to only those employees who require it to perform their job functions. We use industry-standard Secure Socket Layer (SSL) encryption technology to safeguard the account registration process and sign-up information. Self-registration may be available to create new Organizations and new Individuals at existing organizations, but these Individuals do not have administrative access to existing Organizations. Other security safeguards include but are not limited to data encryption and firewalls.

In the event of a data breach: If our Solutions are compromised by an unauthorized individual, we will notify any impacted Organizations as soon as commercially reasonable. The notification will include as much information as possible about the nature of the breach and our steps to mitigate the situation.

We use administrative, technical, and physical security measures to help protect your personal information. While we have taken reasonable steps to secure the personal information you provide to us, please be aware that despite our efforts, no security measures are perfect or impenetrable, and no method of data transmission can be guaranteed against any interception or other type of misuse. Any information disclosed online is vulnerable to interception and misuse by unauthorized parties; we cannot guarantee complete security for your personal information.

4. YOUR CHOICES ABOUT YOUR INFORMATION

Account information and settings: Organizations may update account information and modify Solutions by signing into an administrative account. Organizations and their authorized users can opt out of receiving communications by changing their Account Settings after login or during registration.

If you have any questions about reviewing or modifying account information, contact us directly at support@High5.ID.

Access to Individual Data: Some Individual Data is provided and controlled by their Organizations. If you have any questions about reviewing, modifying, or deleting personal information of an Individual, please contact your Organization directly.

Deleting or disabling cookies: You may be able to disallow cookies to be set on your browser. Please look for instructions on how to delete or disable cookies and other tracking/recording tools on your browser's technical settings. You may not be able to delete or disable cookies on certain mobile devices and/or certain browsers. For more information on cookies, visit www.allaboutcookies.org. Remember, disabling cookies may disable many of the features available on the Solutions, so we recommend you leave cookies enabled.

How long we keep User Content: Following termination or deactivation of a Organization account, High5.ID may retain profile information and content for a commercially reasonable time for backup, archival, or audit purposes. Organizations may set the policy for retention of Individual Data at their own discretion. We may maintain anonymized or aggregated data, including usage data, for analytics purposes. If you have any questions about data retention or deletion, please contact your Organization or support@High5.ID.

5. CHILDREN'S PRIVACY

Individual Data related to children under the age of 13 may be received during the use of our Solutions by an Organization.

High5.ID does not knowingly collect any information from children under the age of 13 unless the Organization has obtained appropriate parental consent for the Individual to use the Solutions or have their data accessible within the Solutions. Please contact us at support@High5.ID if you believe we

have inadvertently collected personal information of a child under 13 without proper parental consents so that we may delete such data as soon as possible.

6. CHANGES TO OUR PRIVACY POLICY

High5.ID may modify or update this Privacy Policy from time to time so you should review this page periodically. If we change the policy in a material manner, for example if we seek to use personal information in a materially different way than we had previously, we will provide at least 30 days' notice to our Organizations so that you have sufficient time to evaluate the change in practice. Of course, you can always opt-out by choosing to deactivate your account before the changes take effect.

7. HOW TO CONTACT US

If you have any questions about this Privacy Policy or the Solutions, please contact us at:

| | |
|-------------------|---|
| Name: | Support Staff |
| Address: | 4219 S Market Ct, Sacramento, CA, USA 95834 |
| Telephone Number: | (833) 847-7277 |
| Email Address: | support@High5.ID. |

High5.ID Security Statement

Last updated: 2020 10 13. Effective Date: 2020 10 13

1. Definitions

- ACCOUNT
 - Credentials and associated licenses enabling an ORGANIZATION to operate HIGH5
- CONTRACT
 - A formal agreement between HIGH5.ID COMPANY and the ORGANIZATION
- CONTRACT COMPLETION
 - The moment when a contract between HIGH5.ID COMPANY and an ORGANIZATION terminates
- DEVICE
 - A computing device, including mobile phone and desktop systems.
- DIY CAPTURE PAGE
 - A web page enabling an INDIVIDUAL to “Do It Yourself” capture a photograph and other information, for example to create an ID card or a yearbook mug shot
- HIGH5.ID COMPANY
 - The publisher of HIGH5.ID
- HIGH5 SERVER
 - The physical location of the code and database accessed by HIGH5
- INDIVIDUAL
 - A person whose information is stored by HIGH5
- INDIVIDUAL DATA
 - Information uniquely associated with a specific INDIVIDUAL
- INDIVIDUAL-GENERATED CONTENT
 - Data created by INDIVIDUALS other than INDIVIDUAL RESPONSES
- KIOSK
 - A physical HIGH5 installation at a POE
- LICENSE
 - A token enabling use of a set of HIGH5 features. Licenses typically expire or count down to zero uses remaining.
- LEA ORGANIZATION
 - A Local Educational Agency - a School or District – making use of HIGH5 as a client, as the case may be
- ORGANIZATION
 - The client making use of HIGH5
- ORGANIZATION REPORTS
 - Data exports of various types including Tardy and Visitor Logs, triggered by ORGANIZATION staff
- POE
 - A physical Point Of Entry at an ORGANIZATION
- PARENT
 - An INDIVIDUAL with custody over a STUDENT at an LEA ORGANIZATION, including legal guardians
- PERSONAL LANDING PAGE
 - A web page personalized for a specific INDIVIDUAL, exposed by an ORGANIZATION.
- RECORD
 - Data associated with a specific INDIVIDUAL by HIGH5

- RESPONSES
 - Content created by INDIVIDUALS, including textual responses, photographs taken by HIGH5 or submitted to HIGH5 by INDIVIDUALS
- SOLUTIONS / HIGH5
 - The High5.ID system, encompassing the online databases and code comprising the totality of experiences for end users and administrators
- STUDENT
 - An INDIVIDUAL receiving instruction at an LEA ORGANIZATION, who may be a minor
- STAKEHOLDERS
 - The totality of INDIVIDUALS, ORGANIZATION staff, PARENTS, and RESELLERS
- TEAMMATE / RESELLER
 - A regional representative of High5.ID working directly with an ORGANIZATION

2. Statements

High5.ID hereby states:

1. RECORDS will be used in the following manner:
 - a. Identifying INDIVIDUALS at POE and other ORGANIZATION moments.
 - b. Offering INDIVIDUAL-specific functionality on INDIVIDUAL devices.
 - c. Generating ORGANIZATION REPORTS.
2. RECORDS continue to be the property of and under the control of the ORGANIZATION.
3. No INDIVIDUAL-GENERATED CONTENT is stored by HIGH5
4. RECORDS shall not be retained or available to High5.ID upon completion of agreements with ORGANIZATION.
5. Personally identifiable information in RECORDS will not be used in targeted advertising unless specifically authorized by the ORGANIZATION.
6. HIGH5 will not condition a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to use the system.
7. High5.ID Company does not intentionally gather any information which indicates the citizenship status of INDIVIDUALS. If in the normal course of operations High5.ID Company becomes aware of such status, it will not unilaterally report this information to any third party. High5.ID Company will fully comply with any lawful demand for information made of it by an appropriate authority.

3. Notifications

1. In-application notifications

In compliance with COPPA and other regulations, the following notifications will be visible:

1. on the HIGH5 KIOSK:

Link from the welcome page: [privacy information](#)

Linked content:

The HIGH5 system makes use of information provided by this school to identify students. This information was provided by the school under the terms of a contract which imposes strict confidentiality requirements.

HIGH5 additionally tracks entry and exit events, notes and conditions entered by school administration, and comments entered by the student themselves in response to questions.

This information is presented to the receptionist to aid in decisions to allow entry or exit to students, and to generate reports detailing visits logs.

Adults wishing to review or modify the information collected by this system should present themselves to the receptionist at this school, who may at their discretion comply with your request.

2. on the HIGH5 DIY CAPTURE PAGE:

Before proceeding to capture photographs or providing contact details, the following message is shown:

You must be 13 years or older to proceed.

By submitting a photo, you grant your school the right to reproduce it in ID cards, the yearbook, and other customary school purposes. Please review your photo carefully. Your school, yearbook company, High5.ID and its teammates assume no responsibility for the content of submitted photos.

In order to proceed, the user must click "I am 13 or older".

2. Parent notifications

In compliance with COPPA and other regulations, the following notifications will be suggested to the ORGANIZATION for broadcast to parents:

Our school has adopted the High5.ID ID management system.

This system was installed to enhance safety for our students and staff: it tracks entries and exits from the school and ensures that our administration know who is in the school and can communicate efficiently with community officials in the event of emergency.

The system tracks the same basics as our school information system - your student's name, a photograph, which class they belong to. It tracks when students have been early or late, with the reasons given. It also keeps a record of all adults (volunteers, replacement teachers, visiting parents) who enter the school.

The information collected by the system will not be shared with any third party with the exception of law enforcement, should the need arise.

Use of this system is mandatory for all students and visitors to the school. You are welcome to ask reception for permission to see the records for your student.

COPPA §312.4.c requires explicit parental approval for disclosure of a child's personal information, the ability to opt out of collection, and rules for automatically deleting students whose parents have not provided permission within reasonable delay.

High5.ID suggests that the needs of a security system differ from normal student-oriented websites. It would be impractical and undesirable to have some students recorded in the database and others not. Requiring all students to be listed in the system supports the school's goal of security.

4. RECORD contents

1. HIGH5 Required Information for all INDIVIDUALS

- Last Name
- First Name
- Role (student, staff, visitor...)

2. HIGH5 Preferred Information for INDIVIDUALS

- Photograph
- Student ID Number (corresponding with Student's permanent record)
- Grade
- Teacher
- ASB membership
- SMS-enabled mobile number
- Email Address
- Digital ID status
- In-person Admissibility

3. HIGH5 Optional Information

- Status at organization
- Date of birth
- Guardian email address
- Guardian SMS-enabled mobile number
- Title
- Company Name

- Group
- Section
- Department
- Personal Government ID Number (typically a drivers license)
- RFID Code
- PURL for individual in RESELLER website
- Locker Number & combination

4. HIGH5 History Baseline

- Flags
- Notes (custody, behavior, etc)
- HIGH5 History Optional information (based on use of additional solutions)
 - Entrance and Exit history
 - Reasons supplied for ingress or egress
 - Results of Sex Offender Database lookups
 - Attendance at courses
 - Presence at school-related events
 - Bus usage history

5. Information & Data Security

1. RECORDS are protected physically:

- No information is stored on-site at the ORGANIZATION except transient browser caches; all information resides on the HIGH5 SERVER. There is no database present on ORGANIZATION hardware.
- Physical locations for the HIGH5 SERVER are:
 - For our domain (hosting and serving of pages) and for maintenance scripts: We use GreenGeeks in California, USA. Physical security measures are in place to prevent unauthorized entry to the site.
 - For our database: we use Google Firebase Realtime Database, a cloud-based system which stores data in central U.S. locations.

2. RECORDS are protected Electronically:

- All communications between the HIGH5 KIOSK and the HIGH5 SERVER are encrypted end-to-end via SSL.
- Hosting and database structures run on a secure host that restricts external access via High5word. Access tokens for the database are encrypted and persisted locally as cookies, a common and trusted approach to security.
- In addition to the userID/password, we use Firebase's support for pre-shared public/private keys to access any infrastructure. Even if someone gets the user ID / High5word pair, they will be unable to access our database from a custom application because the public key is bound to our specific application.

3. Application design:

- HIGH5 uses Firebase, a BaaS (backend-as-a-service) headless server providing secure and encrypted access to connected clients based on
 - a set of rules (e.g. Organization A has access to its own students/staff but does not have access to individuals from Organization B)
 - access tokens (e.g. encrypted local copies of the credentials saved as cookies). These tokens are recycled according to browser configuration. Clearing caches will also invalidate the cookies.

- Firebase is offered by Google, which provides world class security to ensure that unauthorized access is prevented. Details can be found here:
 - <https://firebase.google.com/docs/database/security/>
- The Firebase database supports automatic demand-based server scaling (both physical resources such as RAM and CPU power, and data such as the number of individuals tracked by the database); this enables HIGH5 to dynamically handle as many users as required.
- A maintenance server using Apache and PHP runs clean up and maintenance scripts at regular intervals; these are hosted and run on our servers. Example scripts include: closing visits for individuals that checked in but did not check out; flagging individuals who were late multiple times; and analytics to create daily reports to be sent to ORGANIZATION staff.
- We make use of Firebase's alert systems to monitor system logs and ensure system uptime and performance.
- The database is backed up daily to ensure that logs and records are not lost in the event of catastrophic failure or application error.
- The front end is written in HTML and Javascript.
- Images are served to the client browser using obscured URLs to enhance image security. These URLs cannot be predicted or reverse engineered in order to gain access to other images.
- As with all database access, intruders cannot access images via the database without a secret key which is held by High5.ID alone in a secure location.

6. Instructions and Procedures

1. Actions taken to ensure the security and confidentiality of RECORDS

- a. HIGH5.ID COMPANY staff are designated able to view and modify all RECORDS as required in the accomplishment of their assigned tasks.
- b. RESELLER staff are designated able to view and modify RECORDS for the ORGANIZATIONS as required in the accomplishment of their assigned task for ORGANIZATIONS that they directly service.
- c. HIGH5.ID COMPANY staff are trained to avoid
 - i. Sharing credentials by any means other than password-protected online documentation
 - ii. Releasing private information on ORGANIZATION visitors, staff, students or policies to anyone not associated with the administration of the ORGANIZATION

2. Procedures for notifying STAKEHOLDERS in the event of an unauthorized disclosure of RECORDS

- a. HIGH5.ID COMPANY maintains contact information for administrators at all ORGANIZATIONs and RESELLERS.
- b. HIGH5.ID COMPANY will notify these same by email in the event that unauthorized disclosure takes place. The email will include phone and email information to enable STAKEHOLDERS to contact HIGH5.ID COMPANY staff directly with their concerns.

3. Removal of RECORDS

- a. At CONTRACT COMPLETION, unless otherwise instructed by one or more of the STAKEHOLDERS, HIGH5.ID COMPANY staff will remove RECORDS from
 - i. 'live' database, within 72 hours
 - ii. backups of the database, within 60 days

4. Demonstration that RECORDS have not been retained after contract completion
 - a. At CONTRACT COMPLETION, staff from ORGANIZATION have the right to watch via screensharing technology as HIGH5.ID COMPANY staff clear RECORDS. ORGANIZATION staff will have the opportunity to test that their live database is empty prior to the termination of the ACCOUNT for the ORGANIZATION.

5. Viewing of RECORDS (“right of access”)

- a. Regarding the viewing of RECORDS at a given ORGANIZATION:
 - i. The following may view all INDIVIDUALS:
 1. ORGANIZATION staff
 2. RESELLER staff
 3. HIGH5.ID COMPANY staff
 - ii. The following may, at the ORGANIZATION’S discretion, view their own records:
 1. PARENTS and INDIVIDUALS

3. Correction of RECORDS (“right of rectification”)

- a. Regarding the modification of RECORDS at a given ORGANIZATION:
 - i. The following may modify all INDIVIDUALS:
 1. ORGANIZATION staff
 2. RESELLER staff
 3. HIGH5.ID COMPANY staff
 - ii. The following may, at the ORGANIZATION’S discretion, modify aspects of their own records:
 1. PARENTS and INDIVIDUALS

1. Removal of RECORDS (“right to be forgotten”)

- a. Regarding the erasure of RECORDS at a given ORGANIZATION:
 - i. The following may erase all INDIVIDUALS:
 1. ORGANIZATION staff
 2. RESELLER staff
 3. HIGH5.ID COMPANY staff
 - ii. The following have no means to remove RECORDS:
 1. PARENTS and INDIVIDUALS

2. Business Events

- a. In the event of the sales of all or a portion of the assets of High5.ID, RECORDS may be transferred to the successor entity.
- b. In the event of bankruptcy of High5.ID, RECORDS will not be considered as an asset that can be acquired by a third party.
- c.

===== ENDS =====

High5.ID Terms Of Use – Consolidated

Last updated: 2020 06 29. Effective Date: 2020 09 17.

Welcome to High5.ID! Please enjoy using our technology, but note that your use of it is subject to your agreement with these Terms of Service. This document describes in detail your rights and our rights relating to the provision of the Service (as defined below) so please review these Terms carefully.

By using our Service, you accept these terms and conditions in full. If you disagree with these Terms and Conditions or any part of these Terms and Conditions, you must not use our Service.

Contents:

- Terms of Use - General
- Terms of Use – School Addendum

Please also see our Privacy Policy and our Security Statement. In case of disagreement between these documents, the present Terms And Conditions shall prevail.

Definitions

- ACCOUNT
 - Credentials and associated licenses enabling an ORGANIZATION to operate HIGH5
- CONTRACT
 - A formal agreement between HIGH5.ID COMPANY and the ORGANIZATION
- CONTRACT COMPLETION
 - The moment when a contract between HIGH5.ID COMPANY and an ORGANIZATION terminates
- DEVICE
 - A computing device, including mobile phone and desktop systems.
- HIGH5.ID COMPANY
 - The publisher of HIGH5.ID
- HIGH5 SERVER
 - The physical location of the code and database accessed by HIGH5
- INDIVIDUAL
 - A person whose information is stored by HIGH5
- INDIVIDUAL DATA
 - Information uniquely associated with a specific INDIVIDUAL
- INDIVIDUAL-GENERATED CONTENT
 - Data created by INDIVIDUALS other than INDIVIDUAL RESPONSES
- KIOSK
 - A physical HIGH5 installation at a POE
- LICENSE

- A token enabling use of a set of HIGH5 features. Licenses typically expire or count down to zero uses remaining.
- LEA ORGANIZATION
 - A Local Educational Agency - a School or District – making use of HIGH5 as a client, as the case may be
- ORGANIZATION
 - The client making use of HIGH5
- ORGANIZATION REPORTS
 - Data exports of various types including Tardy and Visitor Logs, triggered by ORGANIZATION staff
- POE
 - A physical Point Of Entry at an ORGANIZATION
- PARENT
 - An INDIVIDUAL with custody over a STUDENT at an LEA ORGANIZATION, including legal guardians
- RECORD
 - Data associated with a specific INDIVIDUAL by HIGH5
- RESPONSES
 - Content created by INDIVIDUALS, including textual responses, photographs taken by HIGH5 or submitted to HIGH5 by INDIVIDUALS
- SOLUTIONS / HIGH5
 - The High5.ID system, encompassing the online databases and code comprising the totality of experiences for end users and administrators
- STUDENT
 - An INDIVIDUAL receiving instruction at an LEA ORGANIZATION, who may be a minor
- STAKEHOLDERS
 - The totality of INDIVIDUALS, ORGANIZATION staff, PARENTS, and RESELLERS
- TEAMMATE / RESELLER
 - A regional representative of High5.ID working directly with an ORGANIZATION

Terms of Use – General

1. Overview

High5.ID is a bundle of solutions provided by Excel Photographers, a California Corporation located in Sacramento, CA. The following explains and define the terms by which Organizations (referred to as “you”) may use our Software and Solutions (referred to as the “Solutions”). If you have questions about this Agreement, please contact sales@high5.id.

This Terms of Use agreement (Referred to as “TOU”) applies to Organizations that use the Solutions, and governs the actions of individuals associated with those Organizations. Local Educational Agencies (LEA) have additional terms of use, included in the TOU – School Addendum.

2. Authority

When you create High5.ID account on behalf of an Organization, then (a) “you” includes you and that Organization, and (b) you represent and warrant that you are an authorized representative of the Organization with the authority to bind the Organization to this Agreement and that you agree to this Agreement on the entity’s behalf.

If you are accessing and using High5.ID on someone else’s behalf, you represent that you have the authority to bind that person as the principal to these Terms, and to the extent you do not have such authority you agree to be bound to these Terms and to accept liability for harm caused by any wrongful use of the Website resulting from such access or use. In such a scenario, the words "you" and "your" when used in these Terms will apply to the entity on whose behalf you are acting as well as you as an individual as appropriate.

If you are using our Services on behalf of a corporate entity or organization, then you agree to these Terms on behalf of that corporate entity or organization and its affiliates and you represent that you have the authority to do so. In such a scenario, the words "you" and "your" when used in these Terms will apply to your or organization and its affiliates as well as you as an individual as appropriate.

3. Permission and grant of license

By using the Solutions, and by logging onto our website you are affirmatively stating your desire to use the Solutions, you signify that you have read, understood, and agree to be bound by this Agreement and to the collection and use of your information as set forth in our Privacy Policy; otherwise you may not use the Solutions.

Only users that are allowed to form a binding contract with High5.ID are allowed to accept these Terms of Use.

Subject to the terms and conditions of this Agreement, we grant you a non-exclusive, limited, non-transferable, freely revocable license to use the Solutions. We reserve all rights not expressly granted to you as defined below.

4. Termination

We may terminate this license at any time for any or no reason. Commercially reasonable restitution will be made for any unused portion of fees paid, in amounts not exceeding the total fees collected by us from you.

5. Account Stewardship

You are responsible for any activity that occurs on your account. You may never use someone else's account without permission, and you must keep your account password secure. We are not liable for any losses of any kind caused by any unauthorized use of your account.

6. Permission to contact

By providing your email address to us you consent to our using the email address to send you Solutions-related notices, including any required legal notices and other messages, such as additions or changes to the Solutions and/or notices of product offers.

7. Modifications

We may modify these Terms from time to time. We will attempt to notify you via the email address you have provided us with, although we are not obliged to. It is therefore important that you review these Terms regularly to ensure you are updated as to any changes.

Upon making changes, we will update the "Effective Date" found at the top of this page. Continued use of the Solutions after notification of any changes constitutes your acceptance of the new terms.

8. Pricing

We reserve the right to modify our prices at any time, subject to our provision of at least six (6) months written notice to you.

9. Suitable devices

Although we make commercially reasonable efforts to provide compatibility with current and recent devices, accessing the Solutions via older or non-standard devices may provide unsatisfactory results.

10. PROHIBITIONS

You are restricted from doing anything to harm our product or try to hack our service. Specifically, by using the Solutions, you agree not to do any of these things: (i) copy, distribute, or disclose any part of the Solutions in any medium, including but not limited to by any automated or non-automated "scraping"; (ii) use any automated system, including but not limited to "robots," "spiders," "offline readers," etc., to access the Solutions in a manner that sends more request messages to the High5.ID servers than a human can reasonably produce in the same period of time by using a conventional online web browser; (iii) transmit spam, chain letters, or other unsolicited email; (iv) attempt to interfere with, compromise the system integrity or security or decipher any transmissions to or from the servers running the Solutions; (v) take any action that imposes, or may impose an unreasonable or disproportionately large load on our infrastructure; (vi) upload invalid data, viruses, worms, or other software agents through the Solutions; (vii) collect or harvest any third-party personally identifiable information, including account names or Individual Data, from the Solutions;

(viii) use the Solutions for any commercial solicitation purposes; (ix) impersonate another person or otherwise misrepresent your affiliation with a person or entity, conducting fraud, hiding or attempting to hide your identity; (x) interfere with the proper working of the Solutions; (xi) access any content on the Solutions through any technology or means other than those provided or authorized by the Solutions; or (xii) bypass the measures we use to prevent or restrict access to the Solutions, including but not limited to features that prevent or restrict use or copying of any content or enforce limitations on use of the Solutions or related content.

If this Agreement ends you continue to be bound by it in any interactions, you may have with the Solutions.

11. Quality of Service / Continuation of Service

We continually update our Solutions to offer the best possible product. While we plan to continue to offer and improve our Solutions, we may, without prior notice, change, cancel, create usage limits for, or permanently or temporarily stop offering or allowing you access to the Solutions generally (“Service Changes”). While we’ll try to give you advance notice of Service Changes that will adversely affect you, this might not be practical or possible and we retain the right to make Service Changes without notice or liability for any reason.

12. CONTENT RIGHTS AND RESPONSIBILITIES

“Individual Data” means any information associated with an individual in the Solutions. While we may need to access Individual Data to provide the Solutions to you, you own the Individual Data and remain responsible for it. Individual Data may include “educational records” as defined by the Family Educational Rights and Privacy Act (“FERPA”); see our Schools Terms of Use Policy for more detail.

“Intellectual Property Rights” means all worldwide patent rights, copyright rights, moral rights, rights of publicity, trademark, trade dress and service mark rights, goodwill, trade secret rights and other intellectual property rights as may now exist or hereafter come into existence, and all related applications and registrations, renewals and extensions.

Except for Individual Data, the Solutions and all materials made available to you in connection with them, including, but not limited to, software, images, text, graphics, illustrations, logos, patents, trademarks, service marks, copyrights, photographs, audio, videos, music, and any content belonging to other Users (the “High5.ID Content”), and all related Intellectual Property Rights, are the exclusive property of High5.ID and its licensors. Except as specified in this Agreement, nothing may be deemed to create a license in or under any such Intellectual Property Rights, and you agree not to sell, license, rent, modify, distribute, copy, reproduce, transmit, publicly display, publicly perform, publish, adapt, edit or create derivative works from any High5.ID Content. To be clear: any use of High5.ID Content for a purpose not expressly permitted by this Agreement is strictly prohibited.

13. Feedback

If you send us ideas or comments about our Solutions, you agree that we may freely use or reference those ideas and comments and we do not owe you any payment or have any other

obligation of any kind for such ideas or comments.

14. High5.ID DATA

Certain parts of the Solutions may allow you to obtain or access analytics or other data or information associated with your account (“High5.ID Data”). High5.ID Data is licensed to you for your use on a limited basis and is governed solely by the terms of this Agreement and available for distribution only at our sole discretion. High5.ID owns the account you use to access the Solutions along with any rights of access or rights to data stored by or on behalf of High5.ID on High5.ID servers (except with respect to any Individual Data that we may be storing for you), including but not limited to any data representing any or all of your High5.ID Data. High5.ID has the right to manage, control and even eliminate High5.ID Data, except that High5.ID may only use Individual Data as specifically permitted by this Agreement.

YOU UNDERSTAND AND AGREE THAT ANY DATA, ACCOUNT HISTORY AND ACCOUNT CONTENT RESIDING ON HIGH5.ID’S SERVERS MAY BE DELETED AT ANY TIME FOR ANY REASON IN HIGH5.ID’S SOLE DISCRETION, WITH OR WITHOUT NOTICE AND WITH NO LIABILITY OF ANY KIND. WE DO NOT PROVIDE OR GUARANTEE, AND EXPRESSLY DISCLAIM, ANY VALUE, CASH OR OTHERWISE, ATTRIBUTED TO ANY DATA RESIDING ON HIGH5.ID’S SERVERS.

15. SECURITY AND PRIVACY

By using the Solutions you consent to the collection, use and disclosure of your information (including but not limited to Individual Data) as set forth in our [Privacy Policy](#) and, if you’re a School, in the Schools Terms of Use, and to have your information (including but not limited to Individual Data) collected, used, transferred to and processed pursuant to our [Privacy Policy](#).

16. THIRD-PARTY INTERACTIONS

Our website may contain links to third-party websites or other materials or information that are not owned or controlled by us. For example, we use a third party to look up sex offenders. We do not endorse or assume any responsibility for any third-party sites, information, materials, products, or Solutions. If you access a third party website, you do so at your own risk; this Agreement, the Schools Terms of Use Information, and our [Privacy Policy](#) do not apply to your use of those sites or Solutions—those sites and Solutions have their own applicable terms and policies.

17. RESPONSIBILITY TO INDEMNIFY

You agree to defend, indemnify and hold harmless High5.ID and its subsidiaries, agents, licensors, managers, and other affiliated companies, and their employees, contractors, agents, officers and directors, from and against any and all claims, damages, obligations, losses, liabilities, costs or debt, and expenses (including but not limited to attorney’s fees) arising from: (i) use of and access to the Solutions by yourself or any Individual affiliated with your Organization, including any data or content transmitted or received by same; (ii) your

violation of any term of this Agreement, including but not limited to your breach of any of the representations and warranties above; (iii) your violation of any third-party right, including but not limited to any right of privacy or intellectual property rights; (iv) your violation of any applicable law, rule or regulation, including but not limited to COPPA; (v) any content or information that is submitted via your account; or (vi) any other party's access and use of the Solutions with your unique username, password or other appropriate security code.

18. DISCLAIMER OF WARRANTY

THE SOLUTIONS IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. USE OF THE SOLUTIONS IS AT YOUR OWN RISK. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SOLUTIONS IS PROVIDED WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. WITHOUT LIMITING THE FOREGOING, HIGH5.ID, ITS SUBSIDIARIES, ITS AFFILIATES, AND ITS LICENSORS DO NOT WARRANT THAT THE CONTENT IS ACCURATE, RELIABLE OR CORRECT; THAT THE SOLUTIONS WILL MEET YOUR REQUIREMENTS; THAT THE SOLUTIONS WILL BE AVAILABLE AT ANY PARTICULAR TIME OR LOCATION, UNINTERRUPTED OR SECURE; THAT ANY DEFECTS OR ERRORS WILL BE CORRECTED; OR THAT THE SOLUTIONS IS FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS. ANY CONTENT DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF THE SOLUTIONS IS DOWNLOADED AT YOUR OWN RISK AND YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR LOSS OF DATA THAT RESULTS FROM SUCH DOWNLOAD OR YOUR USE OF THE SOLUTIONS.

WE DO NOT WARRANT, ENDORSE, GUARANTEE, OR ASSUME RESPONSIBILITY FOR ANY PRODUCT OR SOLUTIONS ADVERTISED OR OFFERED BY A THIRD PARTY THROUGH THE SOLUTIONS OR ANY HYPERLINKED WEBSITE OR SOLUTIONS (INCLUDING WITHOUT LIMITATION APPLICATIONS), AND WE WILL NOT BE A PARTY TO OR IN ANY WAY MONITOR ANY TRANSACTION BETWEEN YOU AND THIRD-PARTY PROVIDERS OF PRODUCTS OR SOLUTIONS (INCLUDING WITHOUT LIMITATION DEVELOPERS). FEDERAL LAW, SOME STATES, PROVINCES AND OTHER JURISDICTIONS DO NOT ALLOW EXCLUSIONS AND LIMITATIONS OF CERTAIN IMPLIED WARRANTIES, SO SOME OF THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

19. LIABILITY LIMITATIONS

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL HIGH5.ID, ITS AFFILIATES, AGENTS, DIRECTORS, EMPLOYEES, SUPPLIERS OR LICENSORS BE LIABLE FOR ANY INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES, INCLUDING WITHOUT LIMITATION DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, DATA OR OTHER INTANGIBLE LOSSES, THAT RESULT FROM THE USE OF, OR INABILITY TO USE, THE SOLUTIONS. UNDER NO CIRCUMSTANCES WILL HIGH5.ID BE RESPONSIBLE FOR ANY DAMAGE, LOSS OR INJURY RESULTING FROM HACKING, TAMPERING OR OTHER UNAUTHORIZED

ACCESS OR USE OF THE SOLUTIONS OR YOUR ACCOUNT OR THE INFORMATION CONTAINED THEREIN.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, HIGH5.ID ASSUMES NO LIABILITY OR RESPONSIBILITY FOR ANY (I) ERRORS, MISTAKES, OR INACCURACIES OF CONTENT; (II) PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, RESULTING FROM YOUR ACCESS TO OR USE OF THE SOLUTIONS; (III) ANY UNAUTHORIZED ACCESS TO OR USE OF OUR SECURE SERVERS AND/OR ANY AND ALL PERSONAL INFORMATION STORED THEREIN; (IV) ANY INTERRUPTION OR CESSATION OF TRANSMISSION TO OR FROM THE SOLUTIONS; (V) ANY BUGS, VIRUSES, TROJAN HORSES, MALWARE OR THE LIKE THAT MAY BE TRANSMITTED TO OR THROUGH THE SOLUTIONS BY ANY THIRD PARTY; (VI) ANY ERRORS OR OMISSIONS IN ANY CONTENT OR FOR ANY LOSS OR DAMAGE INCURRED AS A RESULT OF THE USE OF ANY CONTENT POSTED, EMAILED, TRANSMITTED, OR OTHERWISE MADE AVAILABLE THROUGH THE SOLUTIONS; AND/OR (VII) ORGANIZATION CONTENT OR THE DEFAMATORY, OFFENSIVE, OR ILLEGAL CONDUCT OF ANY THIRD PARTY. IN NO EVENT SHALL HIGH5.ID, ITS AFFILIATES, AGENTS, DIRECTORS, EMPLOYEES, SUPPLIERS, OR LICENSORS BE LIABLE TO YOU FOR ANY CLAIMS, PROCEEDINGS, LIABILITIES, OBLIGATIONS, DAMAGES, LOSSES OR COSTS IN AN AMOUNT EXCEEDING THE AMOUNT YOU PAID TO HIGH5.ID HEREUNDER OR \$100.00, WHICHEVER IS GREATER.

THIS LIMITATION OF LIABILITY SECTION APPLIES WHETHER THE ALLEGED LIABILITY IS BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER BASIS, EVEN IF HIGH5.ID HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. THE FOREGOING LIMITATION OF LIABILITY SHALL APPLY TO THE FULLEST EXTENT PERMITTED BY LAW IN THE APPLICABLE JURISDICTION. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS AGREEMENT GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE. THE DISCLAIMERS, EXCLUSIONS, AND LIMITATIONS OF LIABILITY UNDER THIS AGREEMENT WILL NOT APPLY TO THE EXTENT PROHIBITED BY APPLICABLE LAW.

You are fully responsible for your interactions with other Users, and we have no liability for your interactions with any other Users, or for any User's actions or inactions with respect to you.

20. LAWS GOVERNING THE SOLUTIONS

You agree that: (i) the Solutions will be deemed solely based in California; and (ii) the Solutions will be deemed passive Solutions that do not give rise to personal jurisdiction over us, either specific or general, in jurisdictions other than California. This Agreement will be governed by the laws of the State of California, without respect to its conflict of laws principles. The application of the United Nations Convention on Contracts for the International Sale of Goods does not apply. You agree to submit to the personal jurisdiction of the federal and state courts located in Riverside County, California for any actions related to this Agreement.

21. ADDITIONAL INFORMATION

This Agreement, and any rights and licenses granted hereunder, may not be transferred or assigned by you, but may be assigned by us in accordance with the terms of our [Privacy Policy](#). This Agreement, together with any amendments and any additional agreements you may enter into with High5.ID in connection with the Solutions including other agreements referenced herein, constitute the entire agreement between you and High5.ID concerning the Solutions. If any provision of this Agreement is deemed invalid by a court of competent jurisdiction, the invalidity of such provision will not affect the validity of the remaining provisions of this Agreement, which will remain in full force and effect. No waiver of any term of this Agreement will be deemed a further or continuing waiver of such term or any other term, and High5.ID's failure to assert any right or provision under this Agreement will not constitute a waiver of such right or provision. If access to the Solutions is licensed to the United States government or any agency thereof, or any state or county then the Solutions will be deemed to be "commercial computer software" and "commercial computer software documentation," pursuant to DFARS Section 227.7202 and FAR Section 12.212, respectively, as applicable. Any use, reproduction, release, performance, display, or disclosure of the Solutions and any accompanying documentation by the U.S. Government will be governed solely by this Agreement and is prohibited except to the extent expressly permitted by this Agreement.

Terms of Use – School Addendum

If and only if you are a LEA, the following applies to you.

"Student Data" means "Individual Data" associated specifically with individuals attending your LEA. By using the Solutions provided by High5.ID, you authorize us to receive Student Data or other information via entry or file from registered Organization users.

1. COMPLIANCE WITH APPLICABLE LAWS

Both parties agree to uphold their responsibilities under the Family Educational Rights and Privacy Act ("FERPA"), the Protection of Pupil Rights Amendment ("PPRA"), and the Children's Online Privacy and Protection Act ("COPPA"). We provide the Solutions as an outsourced institutional function under FERPA 34 CFR Part 99.31(a)(1). The Children's Online Privacy and Protection Act ("COPPA") requires that online service providers obtain clear and verifiable parental consent before collecting personal information from children under 13.

YOU REPRESENT AND WARRANT THAT YOU HAVE RECEIVED CONSENT FROM PARENTS OR HAVE THE AUTHORITY TO PROVIDE CONSENT ON BEHALF OF PARENTS, FOR US TO RECEIVE STUDENT DATA RELATED TO CHILDREN UNDER 13.

We recommend that all Schools provide appropriate disclosures to students and parents regarding their use of service providers such as High5.ID and that they provide a copy of our Privacy Policy to parents and guardians.

2. AUTHORIZATION TO ACCESS DATA

A. ACCESS BY US AND OUR AGENTS

As between us, you own all right, title and interest to all Student Data, you are solely responsible for any and all Student Data, whether provided by you, students, or others, and we do not own, control, or license Student Data, except to provide the Solutions.

You authorize High5.ID to store Student Data. We will receive and process Student Data only in order to provide the Solutions.

You authorize High5.ID to access and modify Student Data as may be required in the execution of our work under this agreement.

B. THIRD PARTY ACCESS

We may disclose or provide access to Student Data to our employees and certain service providers with a legitimate need to access such information in connection with providing the Solutions. We and our employees, subcontractors, service providers, or agents involved in the handling, transmittal, and/or processing of Student Data will maintain the confidentiality of any data that includes personally identifiable information and shall not redisclose such data except as necessary in order to provide the Solutions.

C. OTHER ACCESS

Student Data is controlled by LEAs, and we cannot permit anyone else to delete or control Student Data or to transfer such content, or allow access to Student Data by parents or legal guardians; as such, we refer any data access requests to you.

3. HOW WE USE YOUR STUDENT DATA

GRANT OF LICENSE

By submitting Student Data or other information to us, whether via the Solutions or otherwise, you expressly grant, and you represent and warrant that you have all rights necessary to grant, to us a non-exclusive, royalty-free, worldwide license during the term of these Additional Terms and our Terms of Use to use, transmit, distribute, modify, reproduce, display, and store the Student Data only for the purposes of: (i) providing the Solutions as contemplated in these Additional Terms and our Terms of Use, and (ii) enforcing our rights under these Additional Terms and our Terms of Use.

USE OF DATA

We will not use the Student Data for any purpose except as explicitly authorized by these Additional Terms and our Terms of Use. For clarity and without limitation, High5.ID will not use Student Data to engage in targeted advertising.

At your sole discretion, our Associated Agent may be given permission by you to advertise services and products to Students. The default for this option is “permission is not given”.

B. ANONYMIZED DATA

You agree that we may collect and use data derived from Student Data, including data about any Users' access and use of the Solutions, that has been anonymized, aggregated, or otherwise de-identified such that the data cannot reasonably identify a particular student, User, or LEA. We may use such data to operate, analyze, improve or market our Solutions. We will not share or publicly disclose information that is derived from Student Data. We may, track the number of School users on an anonymized aggregate basis as part of our marketing efforts to publicize the total number of Users of the Solutions, and analyze aggregated usage patterns for product development efforts. You further agree that we may use, store, transmit, distribute, modify, copy, display, create derivative works of the anonymized, aggregated Student Data even after this Agreement has expired or been terminated.

4. DELETING STUDENT DATA

You may request in writing that we delete any of your Student Data in our possession at any time. Within seventy-two (72) hours of our receipt of such notice, we will delete all Student Data, except for Student Data residing on backups or internal logs which will be removed within sixty (60) days, and will provide notice to you when Student Data has been deleted.

5. PRIVACY AND SECURITY

If there is any disclosure or access to any personally identifiable Student Data by an unauthorized party, we will promptly notify any affected LEAs and will use reasonable efforts to cooperate with their investigations of the incident. If the incident triggers any third party notice requirements under applicable laws, you agree that, as the owner of the Student Data, you will be responsible for the timing, content, cost, and method of any required notice and compliance with those laws.

IMPORTANT: As a School, you should be absolutely sure to keep secure copies of Student Data in your Student Information System ("SIS") or in other secure storage. You should not rely on us to provide copies of or access to your Student Data. High5.ID does not interact or interface with your SIS for any data transfer unless specifically requested by you and allowed by your SIS provider.