Innive K12 360° Privacy Policy

This is the Innive Inc (Innive) Privacy Policy for the Innive K12 360° solution, as well as any future solutions from Innive or its affiliates designed for education users. If you have questions or concerns about this policy, please contact dataprivacy@inniveinc.com.

Innive is committed to safeguarding the privacy and security of customer information. We believe the personal information of our customers and users, and especially of students, is private, and we treat it confidentially. Innive takes appropriate measures to protect and secure all data provided by the customer and data owners. We adhere to all requirements concerning use of student information protected under the Family Educational Rights and Privacy Act (“FERPA”) and applicable State and Federal laws.

Innive contracts directly with school districts, state and county departments of education, and others (“customers”). These customers are the data owners of any data used in Innive solutions. For the purposes of this policy, “users” are end users of the solution, whether students, parents, teachers, or staff. If a user believes any information on K12 360° to be inaccurate, Innive will direct the user to contact the customer, who owns the data, to review and correct the information as needed.

What information do we collect?

We collect and maintain only the information that is necessary to provide the K12 360° solution and services to our customers and their users.

- The vast majority of data that Innive uses is data that is collected by the customer to display information on data dashboards or in student and employee files. This information is provided to Innive by the customer or data owner.
- Innive is a data custodian of data owned and collected by the customer. This could include data from student information systems (SIS), learning management systems (LMS), enterprise resource planning (ERP) systems, employment records, and gradebook applications, among others. Combining and visualizing this data is essential to the Innive product. Customers may also provide third-party data sources, such as state testing data by school.
- For certain offerings, Innive may be given access to Student Data. “Student Data” is any information that is directly related to an identifiable current or former student that is maintained by a school, school district, or related entity or organization, or by us. Student Data may include “educational records” as defined in the Family Educational Rights and Privacy Act (“FERPA”).
- Some interactions with the product may collect data from users and create a data file linking that data to individual accounts.
- Innive collects data on product usage in order to determine how users are interacting with the product, and how Innive can make the product more intuitive. This data is also used to maintain
the security and operation of our products, and for internal reporting and analytics. This data is automatically collected and may include information such as time spent on a page, where a user has clicked, where a user is logging in from, the type of device or browser being used, IP address, language preferences, operating system, and any errors that the user has encountered.

How do we use your information?

Innive aggregates data that a customer produces across its student information systems, finance and payroll system, and many other systems, brings that data into a single information model, and populates the dashboards and pages of the K12 360° solution with role-based views of the data so support the customer’s goals of improving student learning outcomes and school district/school operations.

Additionally, Innive uses product usage data to determine how users are interacting with the product, and how Innive can make the product more intuitive. This data is anonymized and not connected to any one individual account, but instead gives our team the ability to see how users are interacting with different features of the product and where they might be encountering problems.

Other uses for the collected information include:
- Assistance in account creation or validation, and for the management of user accounts
- Protection of your data
- Responses to legal requests or to prevent harm
- Enforcement of terms, policies, or contracts

Will your information be shared with anyone?

Innive protects users’ rights and security. Data will only be shared with the customer’s consent to deliver solutions or services, or to comply with legal and business obligations. We do not sell, trade, lease or loan student personal information to any third party for any reason, including for marketing or advertising.

We may share data in the following ways:
- As needed to perform the Service and/or at the direction of a Customer and as authorized by our contract with the Customer.
- With our trusted vendors, third party service providers and other individuals who perform services on our behalf, but only if such providers have a need to access such information for the purpose of carrying out their work for us and do so under strict confidentiality and data security terms.
- 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 visitors.
- In the event of a change of control: If we sell, divest or transfer the business or a portion of our business, we may transfer information, provided that the new provider has agreed to data privacy standards no less stringent than our own. We may also transfer personal information – under the same conditions – in the course of mergers, acquisitions, bankruptcies, dissolutions,
reorganizations, liquidations, similar transactions or proceedings involving all or a portion of our business. In either case, we will use our best efforts to provide customers with notice and an opportunity to opt-out of the transfer of their data by deleting their data and terminating their account.

**Do we use cookies or other tracking technologies?**

Innive may use cookies or other tracking technology. Most browsers accept cookies by default. Users have the right to reject or delete cookies. If a user chooses to reject or delete cookies, this could affect certain functioning of the solution.

**How long is your information kept?**

The period of data retention is outlined in Innive’s agreement with the customer and data owner. If the customer is using the Innive solution for any legally required data reporting, it is the responsibility of the customer to retain that reporting and data throughout the period of the contract.

Customer data is kept in a secure computer environment, i.e. the Innive cloud or the customer’s on-premise environment, at all times. Innive will not make additional copies of the data outside of secure environments and any copies of the data will be treated in the same manner as the original source. Data is not stored on any computer outside of the United States.

At the conclusion of the contract, Innive will return or destroy through a secure deletion process any customer data. The period of data retention is outlined in our agreement with the customer and data owner. Innive will delete data at the customer’s request. If a parent or guardian seeks to make changes to a student record, Innive will direct them to the customer.

**How do we keep your information safe?**

Innive maintains a comprehensive set of security practices that are reasonably designed in accordance with commercial best practices to protect the security, privacy, confidentiality, and integrity of student personal information against risks – such as unauthorized access or use, or unintended or inappropriate disclosure – through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information.

Our services include role-based authorization control functionality to enable our customer account administrator to configure and limit access to student and personal information.

Innive relies on the following safety and security measures and policies: data firewalls, testing default settings, data encryption, encryption of data transfer, antivirus and malware protection, secure systems and applications with regular patching, restricting access to data to authorized persons (also known as role based access), authenticated system access, restriction of physical access to data through secured data locations, tracking and monitoring all data access, testing security processes regularly, security provisions of platform vendors like Google, AWS, Elastic and Azure, and maintaining an information security policy.
As part of its contract, Innive asks all customers to confirm compliance with applicable state and federal laws with regards to data security and privacy. We use reasonable efforts to assist our customers in identifying any known security breach in their systems or processes, but we make no claims or warranties to our customer or to any user for any inability, failure or mistake in connection with such assistance.

Data Breach

If Innive becomes aware of a data breach in which a customer’s data may have been accessed, acquired, or disclosed, we will comply with relevant state and other data breach laws and inform the customer in the most expedient way possible and without unreasonable delay. In the event of a data breach, whether to Innive or the customer’s systems, Innive and the customer will coordinate remediation and disclosure to users. Within 20 calendar days of a breach, Innive will provide a report to the customer with the cause of the breach and actions taken to mitigate the breach and prevent similar incidents in the future.

What are users’ privacy rights?

If a user contacts Innive with a request to review, change, or terminate their account, Innive will direct the user to contact their school or district administrator.

Most browsers accept cookies by default. Users have the right to reject or delete cookies if they prefer. If they choose to reject or delete cookies, this could affect certain functioning of the solution.

Innive does not use personal information or account data for advertising or marketing. Some solution information such as features updates or outages may be sent via email to users of the solution. Users can opt-out of these emails in their account settings.

Student Privacy

Innive collects information from students only at the direction of a customer for the purpose of providing Innive’s Service. Innive relies on each school to obtain consent and provide appropriate disclosure, if necessary, for Innive to collect any student information from students under 13, as permitted by the Children’s Online Privacy Protection Act (COPPA). Please contact us at dataprivacy@inniveinc.com if you believe we have inadvertently collected personal information from a student under 13 without proper consent so that we may delete such information as soon as possible.

Specific information for California Residents

Because Innive does not use or share any data for marketing purposes, California’s Shine the Light Law (California Civil Code Section 1798.83) does not apply.
Changes to the Privacy Policy

Innive may modify or update this Privacy Policy from time to time. When the Privacy Policy changes, we will note the effective date at the top of the document and below in “Date Last Modified.” When we change the policy in a material manner, we will provide notice on the K12 360° solution portal and K12 360° website.

Date Last Modified

This Privacy Policy was last modified April 1, 2020

Contact Information

Please contact Innive with any questions or comments about this Privacy Notice by sending an email to dataprivate@inniveinc.com.