Privacy policy

CrickSoftware

USsales@cricksoft.com Toll-free: 1 866 332 7425 us.cricksoft.com

Contents

Introduction 4
1. Important information and who we are 4
Controller 4
Data Privacy Certifications 4
2. The types of personal data we collect about you 4
3. How is your personal data collected? 5
4. How we use your personal data 7
Legal basis 7
Purposes for which we will use your personal data 8
AI-assisted features 10
Direct marketing 10
Third-party marketing 10
Opting out of marketing 10
Cookies 10
5. Disclosures of your personal data 11
6. International transfers 11
7. Data security 12
8. Data retention 12
How long will you use my personal data for? 12
9. Your legal rights 13
No fee usually required 14
What we may need from you 14
Time limit to respond 14
10. Contact details 14
11. Complaints 14
12. Changes to the privacy policy and your duty to inform us of changes 15
13. Third-party links 15

14. Data Breach policy 15
14.1 Overview 15
14.2 Incident response 15
15. Industry standard certifications 17
1EdTech Data Privacy Certification 17

Introduction

This privacy policy sets out how Crick Software Inc (Crick) uses and protects your personal data when using any of our websites, our apps or our computer software and describes our commitment to safeguarding your data, including compliance with U.S. student privacy laws through our 1EdTech certification.

1. Important information and who we are

Privacy policy

This privacy policy gives you information about how Crick Software Inc collects and uses your personal data through your use of this website, our apps or our computer software, including any data you may provide when you register with us or purchase a product or service.

This policy ensures Crick Software:

- Complies with the data protection law
- Follows good practice
- Protects the rights of staff, customers and suppliers
- Is open about how it stores and processes data
- Protects itself from the risks of a data breach

Controller

Crick Software Inc is the controller and responsible for your personal data (collectively referred to as “Crick”, "we", "us" or "our" in this privacy policy).

Data Privacy Certifications

Crick Software is proud to be certified by 1EdTech for data privacy, demonstrating our compliance with key U.S. laws including COPPA (Children’s Online Privacy Protection Act) and FERPA (Family Educational Rights and Privacy Act). This certification reflects our commitment to protecting personal information, particularly for students and educators.

2. The types of personal data we collect about you

Personal data means any information about an individual from which that person can be identified.

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together as follows:

- **Identity data** includes first name, last name, any previous names, job title, username or similar identifier, title, organization name.
- **Contact data** includes billing address, delivery address, email address and telephone numbers.
- **Demographic information** such as geographic region, address, zip code, preferences and interests.
- **Transaction data** includes details about payments to and from you and other details of products and services you have purchased from us.
- **Technical data** includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, device ID and other technology on the devices you use to access this website or our apps or software.
- **Profile data** includes your username and password for our services, purchases or orders made by you, your interests, preferences, feedback and survey responses.
- **Usage data** includes information about how you interact with and use our website, apps, software products and services.
- **Marketing and communications data** includes your preferences in receiving marketing from us and our third parties and your communication preferences.

We also collect and use aggregated data such as statistical or demographic data which is not personal data as it does not directly (or indirectly) reveal your identity. For example, we may aggregate individuals' Usage Data to calculate the percentage of users accessing a specific feature of our services in order to analyze general trends in how users are interacting with our website and / or products to help improve the website, products and our service offering.

The only student information that we store is the student's email address and basic profile information. This is required to confirm that they are a licensed user.

Crick Software Inc. does not claim ownership of any student or user personal data. All personal data collected is used solely for licensing and service provision purposes. Users retain full ownership of their personal data and may request its deletion at any time. Upon receiving such a request, Crick Software Inc. will delete the data within two business weeks.

We do not scan any content. Text or media entered by the user into our apps is not collected and is not viewable by us.

3. How is your personal data collected?

We use different methods to collect data from and about you including through:

- **Your interactions with us.**
  You may give us your personal data by filling in online forms or by corresponding with us by post, phone,

email or otherwise. This includes personal data you provide when you:

- apply for our products or services;
- complete forms on our website;
- update or add your details to our database;
- create an account on our website, apps or software;
- subscribe to our service or publications;
- request marketing to be sent to you;
- enter a competition, promotion or survey; or
- give us feedback or contact us.

- **Automated technologies or interactions.**
  As you interact with our website, we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. We may also receive Technical Data about you if you visit other websites employing our cookies.

- We automatically collect usage data when you are using our apps or software. This may include how frequently the app or software is used, and which features are used. We never collect, view or store any text or media created by the user in our apps or software.

- If you fill out a web form on our site, your information will be stored in our CRM system and some of your past browsing on our site may be available to us to determine your interests. We may use this information to more effectively engage with you and improve our site. However, if you use private browsing as described below, you may provide us your information without making your past browsing activity available to us. If you do not wish for us to have your personal information, please do not fill out any of the web forms on our site.

- If you provide your email address, we will process your data as “legitimate interest.” If we contact you, some information is collected about when/if the email was opened and what links were clicked. This information is used to assess the engagement and success of an email campaign.

- Clicking on a link in any of these emails may cause you to be personally identified and may cause some part of your past browsing history on our site to be available to us so we may more effectively engage with you and improve our site. If you do not wish for this tracking to occur, you can unsubscribe from our mailings or use private browsing mode to avoid tracking.

- We never use visitor identification techniques that involve sharing information you provide us with other sites or vice versa. We never store any information in your computer’s Flash local shared objects area (i.e., we never use what is known as ‘flash cookies’).

- **Third parties or publicly available sources.**
  We may receive personal data about you from various third parties and public sources as set out below:

- Technical Data is collected from the following parties:
    - analytics providers such as Google;
- Identity and Contact Data is collected from data brokers or aggregators such as EduLead in the US and The Education Company (SPIRIT) based in the UK,– their privacy policies can be viewed via the following links:
    - Privacy Policy - Edulead
    - Privacy Policy | The Education Company

      We only receive data from third-party sources where individuals have lawfully provided their consent or where collection is otherwise compliant with applicable laws
- Our apps and software use Pendo (a software experience management platform) to collect usage data. This may include the frequency of use and the features used. Pendo's privacy policy can be viewed at https://www.pendo.io/legal/privacy-policy/
- **Web apps.**
  Our web apps typically use your Google ID and Google domain as identifiers to authorize your license.
- **User settings and usage data.**
  We may use cookies, local storage and users' Google™ accounts to store user settings and usage information.
- **Required permissions.**
  Applications that integrate with a Google account must declare their intent by requesting permissions. These permissions to your browser and account must be granted in order to integrate with Google accounts. Below is a list of these permissions and why they are required. At no time will Crick Software request or have access to your Google account password.
    - Google Drive
        - View and manage the files in your Google Drive (allows the user to manage their Google Drive files from within the app)
    - Basic account info
        - View your email address (used to identify the user for licensing the app)
        - View your basic profile info
    - Device Camera (allows the app to use the camera when the user wants to insert a picture or video)
- You can revoke these permissions at any time on your Google Account Permissions page, however if you do this, the web apps may cease to work or have reduced functionality

4. How we use your personal data

Legal basis

We rely on one or more of the following legal bases for collecting and using your personal data:

- **Performance of a contract:** Where we need to perform the contract we are about to enter into or have entered into with you.

- **Legitimate interests:** We may use your personal data where it is necessary to conduct our business and pursue our legitimate interests, for example to prevent fraud and enable us to give you the best and most secure customer experience, to carry out direct marketing, develop our products/services and grow our business. We make sure we consider and balance any potential impact on you and your rights (both positive and negative) before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).

- **Legal obligation:** Where it is necessary for compliance with a legal obligation that we are subject to, including US-specific laws such as CCPA.

- **Consent:** Where we have obtained your active agreement to use your personal data for a specified purpose, for example, if you subscribe to an email newsletter or request marketing information.

Purposes for which we will use your personal data

We have set out below, in a table format, a description of all the ways we plan to use the various categories of your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Purpose/Use	Type of data	Legal basis
To register you as a new customer	(a) Identity (b) Contact	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to identify appropriate services for you and manage our relationship with you)
To process and deliver your order including: (a) Manage payments, fees and charges (b) Collect and recover money owed to us	(a) Identity (b) Contact (c) Financial (d) Transaction (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to recover debts due to us)
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy (b) Dealing with your requests, complaints and queries (c) Notifying you about changes to our service	(a) Identity (b) Contact (c) Profile (d) Marketing and Communications	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and manage our relationship with you)

To enable you to complete a survey	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to study how customers use our products/services, to develop them and grow our business)
To improve, administer and protect our business, apps, software and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data) including ensuring that our content is presented in the most effective manner for you and for your device	(a) Identity (b) Contact (c) Technical	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganization or group restructuring exercise) (b) Necessary to comply with a legal obligation
To deliver relevant website content and online advertisements to you and measure or understand the effectiveness of the advertising we serve to you	(a) Identity (b) Contact (c) Profile (d) Usage (e) Marketing and Communications (f) Technical	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, apps, software, products/services, customer relationships and experiences and to measure the effectiveness of our communications and marketing	(a) Technical (b) Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To send you relevant marketing communications and make personalised suggestions and recommendations to you about goods or services that may be of interest to you based on your Profile Data	(a) Identity (b) Contact (c) Technical (d) Usage (e) Profile (f) Marketing and Communications	Necessary for our legitimate interests (to carry out direct marketing, develop our products/services and grow our business). We supply a product that supports children in schools with their literacy and we send details of our products to teachers in our database

To carry out market research through your voluntary participation in surveys	(a) Identity (b) Contact	Necessary for our legitimate interests (to study how customers use our products/services and to help us improve and develop our products and services)

AI-assisted features

Clicker may include optional AI-assisted features designed and provided by Crick Software with safeguards and controls to support teachers in creating educational resources. These features do not require personal data and operate within the existing use of personal data described in this Privacy Policy.

User input is not stored, and is not used to train AI models or LLMs.

Please see our AI Safeguarding Policy for details of the safeguards and controls applied to AI-powered features.

Direct marketing

You will receive marketing communications from us if you have requested information from us or purchased goods or services from us and you have not opted out of receiving the marketing. We may also analyze your Identity, Contact, Technical, Usage and Profile Data to form a view which products, services and offers may be of interest to you so that we can then send you relevant marketing communications.

We will never send marketing communications to student email addresses.

Third-party marketing

We do not sell, rent or share your personal data with third parties for their own direct marketing purposes. Our service providers may only process personal data on our behalf and in accordance with our instructions.

Opting out of marketing

You can ask us to stop sending you marketing communications at any time by following the opt-out links within any marketing communication sent to you. We will remove your details from our email list and will not send you information until or unless you ask us to do so.

If you opt out of receiving marketing communications, you will still receive service-related communications that are essential for administrative or customer service purposes for example relating to order confirmations, appointment reminders, updates to our Terms and Conditions, checking that your contact details are correct.

Cookies

For more information about the cookies we use and how to change your cookie preferences, please see our Cookie policy.

5. Disclosures of your personal data

We may share your personal data where necessary with the parties set out below for the purposes set out in the table above.

- Internally within Crick Software:
    - Crick Software employees will only access content on our servers to manage subscriptions and licensing. The customer information visible to Crick Software employees is:
        - School/organization details
        - School/organization usage information
        - Users' email addresses and basic profile info
        - App usage data (see above)
- External Third Parties:
    - Save for storing data on third party servers, we will not disclose your personal information to any other party other than in accordance with this Privacy Policy unless we are legally required to do so by law.

We require all third parties to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

6. International transfers

We may transfer your personal data to service providers that carry out certain functions on our behalf.

- Your personal data will be stored and processed in the United States. We ensure that appropriate safeguards are in place to protect your personal data in accordance with this privacy policy, applicable US data protection laws, and international standards. These safeguards include secure servers, encrypted databases, and restricted access to personal data.
- We will only transfer your personal data to countries that have been deemed by the US to provide an adequate level of protection for personal data, namely, EU countries and the USA through the EU-US Data Privacy Framework.
- We may use specific standard contractual terms approved for use in the US which give the transferred personal data the same protection as it has in the US, namely the International Data Transfer Agreement or The International Data Transfer Addendum to the European Commission's standard contractual clauses for international data transfers. To obtain a copy of these contractual safeguards, please contact us using the Contact details below (section 10).

7. Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed.

These measures include the use of secure servers, encrypted databases, storage of the information in non-public areas of the servers, and other measures as deemed reasonable and necessary. In addition, once a subscription has expired for more than 24 months, the student personal information is deleted from our records.

We encrypt the transmission of data on pages where you are required to provide payment information.

In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

However, it's important to note that no security or encryption method can be guaranteed to protect information from hackers or human error.

8. Data retention

How long will you use my personal data for?

We will only retain your personal data for as long as reasonably necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

By law we have to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for six years after they cease being customers for tax purposes.

In some circumstances you can ask us to delete your data: see section 9 below for further information.

In some circumstances we may anonymize your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

Save for the exceptions listed above we will usually delete your email address and basic profile info after two years of not using our service.

Users may request deletion of their personal data at any time. Upon such a request, Crick Software Inc. will ensure that all relevant data is deleted from our systems within two business weeks, in accordance with our commitment to user data ownership.

9. Your legal rights

You have a number of rights under data protection laws in relation to your personal data.

You have the right to:

- Request access to your personal data (commonly known as a "subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

- Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

- Request erasure of your personal data in certain circumstances. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

- Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) as the legal basis for that particular use of your data (including carrying out profiling based on our legitimate interests). In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your right to object.

- You also have the absolute right to object any time to the processing of your personal data for direct marketing purposes (see Opting out of marketing in section 4 for details of how to object to receiving direct marketing communications).

- Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

- Withdraw consent at any time where we are relying on consent to process your personal data (see the table in section 4 for details of when we rely on your consent as the legal basis for using your data). However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

- Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in one of the following scenarios:

    - If you want us to establish the data's accuracy;

- Where our use of the data is unlawful but you do not want us to erase it;
- Where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
- You have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

If you wish to exercise any of the rights set out above, see Contact details.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we could refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it could take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

10. Contact details

If you have any questions about this privacy policy or about the use of your personal data or you want to exercise your privacy rights, please contact us in the following ways:

- Email address: support@cricksoft.com
- Postal address: Crick Software, Inc. 100 Technology Drive, Suite 200, Trumbull, CT 06611
- Telephone number: (+1) 203 221 2697

11. Complaints

If you have any concerns about how we handle your personal data, you can contact us using the details provided in section 10. We will investigate and respond to your complaint promptly.

You have the right to make a complaint at any time to the relevant US authorities if you believe your data protection rights have been violated. We would, however, appreciate the chance to deal with your concerns before you approach these authorities, so please contact us in the first.

12. Changes to the privacy policy and your duty to inform us of changes

We keep our privacy policy under regular review. This version was last updated in April 2025. Previous versions can be obtained by contacting us.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us, for example a new address or email address.

13. Third-party links

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy policy of every website you visit.

14. Data Breach policy

14.1 Overview

a. As an organization that processes personal data, Crick Software must ensure appropriate measures are in place to protect against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. The General Data Protection Regulation specifies that all breaches (except those 'unlikely to result in a risk to the rights and freedoms of natural persons') should be reported to the Information Commissioner. In the event of a data breach or an information security incident, it is important that appropriate actions are taken to promptly report the breach using the contact details at clause 10 so we can manage the incident and minimize associated risks. This procedure is designed to set out the process that should be followed to ensure a consistent and effective approach is in place for managing a data breach and ensure that:

   i. Data breach events are detected, reported and monitored consistently
   ii. Incidents are assessed and responded to appropriately
   iii. Action is taken to reduce the impact of a breach
   iv. Relevant breaches are reported to the Information Commissioner within the 72-hour window
   v. Improvements are made to prevent recurrence
   vi. Lessons learned are communicated to the wider organization

14.2 Incident response

a. Despite detailed guidelines for securing confidential electronic data, breaches can still occur. At such times, it is important that Crick Software respond as quickly as possible. Computer thefts or loss should be reported immediately to the line manager. Steps that we will take in the event of a data security breach are

as follows:

i. Determination of the nature and scope of a breach
   A. Identification of the person reporting the breach (name, contact info, etc.)
   B. Record of the location, timeframe, and apparent source of the breach
   C. Preliminary identification of confidential data that may be at risk

ii. Communication
   A. Use the contact details at clause 10;
   B. Notify the police (depending on the nature/scope of theft)

iii. Investigation
   A. Identify ongoing vulnerability of data to exposure from breach source (take immediate steps to address)
   B. Conduct preliminary analysis
   C. Prepare inventory of data at risk
   D. Determine if exposed data were encrypted
   E. Identify security measures that were defeated (and by what means)

iv. Assessment of breach
   A. Identify affected individuals at risk of identity theft or other harm
   B. Assess financial, legal, regulatory, operational, reputational, and other potential institutional risks

v. Remediation
   A. Implement password changes and other security measures to prevent further data exposure
   B. Determine if exposed/corrupted data can be restored from backups; take appropriate steps
   C. Determine if the value of exposed data can be neutralized by changing account access, ID information, or other measures

vi. Notification
   Based on the assessments above, the Data Protection Team will decide whether the breach incident needs to be reported to the ICO or the data subjects. Either way, the breach will need to be added to the breach log to include the following points:
   A. Nature and scope of breach
   B. General circumstances of the breach (e.g., stolen laptop, hacked database, etc.)
   C. Approximate timeline (e.g., date of breach discovery)
   D. Steps that Crick Software has taken to investigate and assess the breach
   E. Any involvement of law enforcement or other third parties
   F. Appraisal of any misuse of the missing data
   G. Steps we are taking to prevent future breaches of this nature

vii. Post-incident follow-up
   Following a data security breach, Crick Software will:
   A. Take steps to ensure that missing data cannot be used to access further information from our servers
   B. Pursue with law enforcement all reasonable means to recover lost data and equipment
   C. Review and modify as needed; all procedures, governing systems, administration, software management, database protections, access to hardware, etc., to prevent future data breaches of a similar nature
   D. Take appropriate actions if staff negligence or other's behavior contributed to the incident

E. Modify procedures, software, equipment, etc. as needed to prevent future data breaches of a similar nature
F. Take appropriate action if personnel negligence caused or contributed to the incident

15. Industry standard certifications

At Crick Software Inc, we are committed to maintaining the highest standards of data protection and security. To demonstrate our commitment, we have obtained the industry-standard 1EdTech Data Privacy Certification.

1EdTech Data Privacy Certification

- We are proud to be certified by 1EdTech, which ensures that our products and services meet rigorous standards for data privacy in the education technology sector. This certification provides assurance that our solutions are designed to protect student data and comply with key US privacy laws, including:

- **Children's Online Privacy Protection Act (COPPA)**: This law imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age.

- **Family Educational Rights and Privacy Act (FERPA)**: This federal law protects the privacy of student education records and gives parents certain rights with respect to their children's education records. These rights transfer to the student when they reach the age of 18 or attend a school beyond the high school level.

These certifications reflect our dedication to providing secure and reliable services to our customers. We continuously review and update our practices to comply with the latest industry standards and regulatory requirements.

For more information about our certifications and what they mean for you, please contact us using the details provided in section 10.

Crick Software Inc.

Last modified: October 2026

CrickSoftware