Privacy Policy

Updated 18-May-23

Introduction

Your privacy is very important to us. This notice describes the personal data we collect, how it is used and shared, and your choices regarding this data. We may occasionally update this notice. We encourage users to periodically review this notice for the latest information on our privacy practices. If you have any questions or concerns about your privacy or anything in this notice, we encourage you to contact us at privacy@connect4education.com.

Applicability of this Notice

This notice describes C4E's personal data collection and usage practices. It applies to all products and services offered by us, and all users of our website, referred to as 'users' in this notice. California users should refer to the specific section of this notice addressing C4E's privacy practices concerning the California Consumer Privacy Act (CCPA).

Data Collection

The following data is collected by or on behalf of C4E:

1. Data provided by users. This data includes:

- Name
- Email address

2. Data created during the use of our services, including:

- Usage data
  We collect data on user interactions with our services, such as access dates and times, pages viewed, system activity, and browser type. We may gather this data through cookies, server logs, plug-ins, and similar tracking technologies that create and maintain unique identifiers. To learn more about these technologies, please refer to our Cookie Policy.
- Device data
  We may collect data about the devices used to access our services, including the hardware models, device IP address and operating systems and versions, as well as software.

Data Usage

C4E collects and uses data to provide our products and services, ensuring reliable and convenient delivery. Additionally, we use the collected data to:

- Grant access to our products and services.
- Facilitate research and development.
- Offer customer support.
- Comply with legal obligations or protect our rights.

C4E does not sell or share personal user data with third parties for marketing purposes.

Data Sharing

C4E may share collected data:

1. With C4E service providers and business partners, including:
    - Payment processors and facilitators
    - Cloud storage providers
    - Data analytics and educational software providers
2. For legal reasons or in the event of a dispute, if required by applicable law, regulation, operating license or agreement, legal process, or governmental request, or when disclosure is appropriate due to safety or similar concerns. This also includes sharing personal data in connection with, or during negotiations of, any merger, sale of company assets, consolidation or restructuring, financing, or acquisition of all or a portion of our business by or into another company.

We do not sell, trade, or rent users' personal identification information to others.

Data Retention

C4E retains user data for as long as necessary for the purposes outlined above. Different data categories are retained for varying periods depending on the user category, data type, and collection purposes. Users may request account deletion by contacting privacy@connect4education.com C4E may retain user data after a deletion request due to legal or regulatory requirements or as stated in this policy.

Grounds for Data Processing

We collect and use personal data only when we have lawful grounds to do so, such as providing requested services and features, for C4E's legitimate interests or those of other parties, to fulfill our legal obligations, or based on consent.

Children's data

C4E is not directed to children, and we do not knowingly collect personal information from children under 13. If we discover that a child under 13 has provided us with personal information, we will take steps to delete that information. If you believe a child under 13 has given us personal information, please contact us at privacy@connect4education.com.

Rights as a California Residents

The California Consumer Privacy Act (CCPA) allows consumers in California to opt out of certain data sharing. It is essential to note that C4E does not sell your data. For more information on the data we collect and how we use it, please refer to the sections above. California law requires us to inform you of our response to web browser Do Not Track (DNT) signals. This setting requests that a web application disable its tracking of an individual user. If you choose to activate the DNT setting in your browser, your browser sends a special signal to websites to stop tracking your activity. Our website does respond to DNT signals.

California residents may request that C4E:

- Disclose the sources, categories, and specific pieces of personal information we have collected about them, as well as how that information is used, its purpose, and with whom C4E shares it.
- Delete their personal information.
- Provide a copy of their personal information in a readily usable format that allows the information to be transmitted to others.

Users Outside of the United States

C4E is located in the United States. If you are a user based outside the United States, be aware that any personal data you provide to us may be stored, processed, transferred between, and accessed from the United States and the country in which you reside. By using our services, you consent to this transfer. We will protect the privacy and security of personal information as set out in this notice, regardless of where it is processed or stored; however, you explicitly acknowledge and consent to the fact that personal data stored or processed in the United States will be subject to the laws of the United States, including the ability of governments, courts, law enforcement, or regulatory agencies of the United States to obtain disclosure of your personal information.

FERPA (Family Education Rights and Privacy Act)

FERPA is a US federal law that protects the privacy of student educational records. We abide by all applicable provisions and guidelines of the FERPA (Family Education Rights and Privacy Act) (20 USC § 1232g; 34 CFR Part 99) as stated in the US Department of Education FERPA page.

Our security and privacy measures include, but are not limited to:

- Protecting data in transit with Transfer Layer Security TLS 1.2 and 256-bit Advanced Encryption Standard (AES-256).
- Adhering to the Payment Card Industry Data Security Standard (PCI DSS) during electronic transactions with students.
- Leveraging the physical and environmental protection of our CoreSite data center provider facilities, implementing 24x7 manned security and monitoring through multiple layers of physical security controls, including perimeter fences, manned lobbies,

surveillance cameras (CCTV), man traps, locked cages, motion detectors, and biometric access requirements.

- Not monitoring, viewing, or tracking the video or audio content of students' communication or assignment submissions.
- Not sharing student data, including all Personally Identifiable Information (PII) and other non-public information, except as required by law, statute, or court order.
- Using only de-identified student data for product development, research, or other purposes, ensuring all direct and indirect personal identifiers are removed.
- Not attempting to re-identify de-identified data and not transferring data to any party unless that party agrees not to attempt reidentification.
- Not using any student data to advertise or market to students or their parents and not using data for any purpose.
- Not engaging in any data mining or scanning activities of user-generated content for advertising or marketing purposes directed towards students or their parents, under any circumstances.
- Ensuring the proper disposal or transfer of all data in our possession or that of our subcontractors or agents, to whom we may have transferred data, to the adopting school under its direction. This process will take place upon request from the adopting school when the data is no longer required for the purpose of providing services to the school.
- Storing and processing data in compliance with industry best practices, implementing appropriate administrative, physical, and technical safeguards to protect data from unauthorized access, disclosure, and utilization.
- Conducting periodic risk assessments and diligently addressing any identified security vulnerabilities in a timely fashion, ensuring the ongoing protection of users' data.
- Notifying the adopting school and adhering to best practices for responding to breaches involving Personally Identifiable Information (PII) in the event of a security or privacy incident. Upon request, C4E agrees to share our comprehensive incident response plan with the adopting school.

Contacting Customer Service

If you wish further information about this Policy or any other C4E Policy, or need assistance, please reach out to C4E Customer Service through the following means:

Connect For Education, Inc.
620 Herndon Parkway, Suite 200
Herndon, VA 20170
(703) 880-1180 x 300
Email: privacy@c4edu.com