

## **CampusClear™ Mobile App Privacy Policy**

Last Modified: July 6, 2020

### **Introduction**

We respect your privacy and are committed to protecting it through our compliance with this Policy. This Policy describes the types of information we may collect from or about you in connection with our CampusClear™ application for your mobile device (our “Application”), and our practices for collecting, using, maintaining, protecting, and disclosing that information.

This Policy applies to any information we collect in connection with our Application. This Policy does not apply to any other information we collect by any other means.

Please read this Policy carefully to understand our policies and practices regarding your information and how we will treat it. If you do not agree with our policies and practices, you can choose not to use our Application. By accessing or using our Application, you agree to this Policy. This Policy may change from time to time. When we make changes to this Policy, we will post the updated Policy on our Application and update the Policy’s “last modified” date. We will also provide notice of any material changes as explained in the section below titled “*Changes to Our Privacy Policy.*” Your continued use of our Application after we make changes is deemed to be acceptance of those changes; provided, however, that we will not collect additional categories of personal information beyond those disclosed in this Policy without providing additional notice to you, and we will not use your personal information for additional purposes beyond those disclosed in this Policy without providing notice and obtaining your consent.

### **Our Role as a Service Provider to Higher Ed Institutions**

The Application is intended to be used as a self-reporting, self-screening tool for symptoms related to the novel coronavirus SARS-CoV-2, the virus that causes COVID-19, for use on the campuses of institutions of higher education in the United States. Colleges, universities or other institutions of higher education may elect to use the Application and related “dashboard” software that we license to them (the “Dashboard Software”) on their campus under contract with us (each such institution, a “Higher Ed Institution”) and, for clarity, “you” are an individual student, faculty member, staff member, visitor, or other constituent of a Higher Ed Institution. We are merely a service provider to the Higher Ed Institution permitting them to use the Application and our Dashboard Software on their campus. We collect information through your use of the Application and process that information on the Higher Ed Institution’s behalf and under the Higher Ed Institution’s control and direction, pursuant to our contract with the Higher Ed Institution. As between you and us, we commit to you that we will collect and process your information in accordance with this Policy, as part of the services we provide to the Higher Ed Institution. However, as between you and the Higher Ed Institution, with respect to information about you that the Higher Ed Institution obtains through your use of the Application, each Higher Ed Institution independently has the right to determine the purposes for which it will process such information and the means the Higher Ed Institution will use to process such information. The Higher Ed

Institution is the “owner” of the information, at least as between us and them. We do not control (and are not responsible for) the applicable Higher Ed Institution’s policies and practices relating to the collection, use, maintenance, protection or disclosure of your information, including information about you that the Higher Ed Institution obtains through your use of the Application. We only control (and are only responsible for) our own actions and the actions of our own service providers, as described in this Policy. We encourage you to review the responsible Higher Ed Institution’s privacy policy or consult with an administrator of the Higher Ed Institution for more information about how the Higher Ed Institution may collect, use, maintain, protect and disclose your information.

### **Information Collected About You and How it is Collected**

We may collect several types of information from and about users of our Application, including information by which users may be personally identified or information about a user that is maintained in personally-identifiable form (collectively “Personal Information”). Specifically:

- *Identifiers*: You provide your first name (or “nickname”) and e-mail address or mobile telephone number when you register to use our Application (collectively, the “Identifiers”); and
- *Health Screening Information*: You provide information about your self-reported symptoms related to COVID-19 (or lack thereof) when you complete and submit a daily self-screening survey through the Application (collectively, the “Health Screening Information”).

Additionally, administrators at Higher Ed Institution may choose to upload certain information about you and associate it with information collected through the Application in a record maintained in the Dashboard Software. This information could include your e-mail address or mobile telephone number in combination with one or more of the following: if you are a student, information about your class schedule and campus housing arrangements, and if you are a faculty member or staff, your department and your work location (building or buildings on campus where you perform your work) (collectively, the “Additional Employment and Education Information”). We encourage you to review the responsible Higher Ed Institution’s privacy policy or consult with an administrator of the Higher Ed Institution for more information about its choices as to the information the Higher Ed Institution is uploading to and processing via the Dashboard Software.

### *Traffic, Usage and Device Information*

Finally, as you navigate through and interact with our Application, we may automatically collect certain traffic data, usage information, and information about your mobile device, such as your mobile device’s operating system, your wireless carrier, configuration data, clickstream analytics and your actions and patterns when you use our Application. The technologies we use for this automatic data collection may include cookies that are stored on your mobile device, small embedded electronic files known as web beacons (also referred to as clear gifs, pixel tags and single-pixel gifs) and other types of embedded code. We collect this information to manage our content and improve users’ use of our Application; count and review the number of users of our Application and their usage patterns; to track key performance indicators such as pages accessed,

frequency of access and other statistical information related to our Application (for example, recording the popularity of certain content and verifying system and server integrity); to identify the portion of users who accesses our Application via iOS or Android; to recognize if user is a return user of our Application; to store information about a user's visits; and to remember a user's preferences.

## **How We Use Your Information**

### *Generally*

We may use the information we collect about you or that you provide to us, including Personal Information, to:

- Create, maintain, customize, and secure your account with us.
- Provide our Application and its contents to you.
- Help maintain the safety, security, and integrity of our Application, databases and other technology assets and our business.
- Notify you about changes to our Application.
- With respect to automatically-collected traffic, usage and device information, fulfill the purposes described in the section above titled "*Traffic, Usage and Device Information.*"
- To store this information on behalf of your Higher Ed Institution and make this information available to your Higher Ed Institution in conjunction with their COVID-19 monitoring and contact tracing efforts.
- Respond to lawful requests for information through court orders, subpoenas, warrants and other legal processes or obligations.
- Enforce any contracts between you and us, or for the establishment, exercise or defense of legal claims.
- Evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Information held by us is among the assets transferred.
- Fulfill any other purpose for which you provide the information.
- Serve any other purpose that we describe when you provide the information and for any other purpose with your consent.

### *Use and Disclosure of Aggregated or De-Identified Data*

We may convert or combine some Personal Information of users into de-identified or aggregated data that does not disclose any of the Personal Information of any individual user. We may use and disclose to third parties any such de-identified or aggregated data (including traffic and usage data that does not identify you personally) for any lawful purpose.

### *Tracking and "Do Not Track"*

Tracking involves the use of cookies, web beacons, or other embedded code or tracking technologies to collect, analyze and store information on a user's behavior over time on multiple

sites, including information on the sites visited, products viewed, products purchased and other online interactions. Tracking information can be used to enable companies to make interest-based (behavioral) advertising available to users on multiple sites that they visit.

We do not currently collect Personal Information about your online activities over time and across third-party sites for tracking purposes. We do not currently allow third parties to collect Personal Information through or using our Application that could be used by them to analyze and store information about your online activities over time and across third-party sites for tracking purposes. Therefore, our Application does not respond to any “do not track” signals sent by your mobile device, and if your mobile device sends a “do not track” signal to our Application, our Application will not treat you differently from users who do not send such signals.

### **Disclosure of Your Information**

#### *Generally*

By registering for and using the Application, you direct us to disclose (and you consent to our disclosure of) the information you provide to us (including, specifically, your Health Screening Information) to your Higher Ed Institution for their use in conjunction with their COVID-19 monitoring and contact tracing purposes and for other purposes determined in their discretion. You should review your Higher Ed Institution’s privacy policy or consult an administrator at your Higher Ed Institution for more information on their use, disclosure and processing of this information.

We do not otherwise share, sell or lease your Personal Information to any third parties, and we only permit use of your Personal Information internally by our own personnel, except in the following, limited circumstances:

- We may disclose Health Screening Information and the Additional Employment and Education Information to any contractors, service providers and other third parties who need to know such information to provide services to us that support our permitted uses of Personal Information under this Policy. For example, we use a third party cloud-hosted IT infrastructure service provider to securely store and maintain the information you provide to us via the Application. We do not disclose Identifiers to such contractors, service providers or other third parties because the Identifiers are maintained in encrypted and pseudonymized (“hashed”) form on our systems and may only be accessed (decrypted) by the Higher Ed Institution through the Dashboard Software.
- We may disclose all types of Personal Information to a buyer or other successor to our business in the event of a sale of equity or assets, reorganization, merger or a similar corporate transaction, and any due diligence review with respect to any such proposed transaction.
- We may disclose all types of Personal Information to comply with any court order, law or legal process, including to meet national security and law enforcement requirements

and to respond to any government or regulatory request or audit, and to enforce or apply our CampusClear™ Licensed Application End User License Agreement (available online at: [\[https://drive.google.com/file/d/1R4GO-e7B4BPlmOfPEUot2IIBkkoLrhp/view?usp=sharing\]](https://drive.google.com/file/d/1R4GO-e7B4BPlmOfPEUot2IIBkkoLrhp/view?usp=sharing)), or if we believe disclosure is necessary or appropriate to protect the rights, property or safety of our customers or others.

We may also disclose your Personal Information for any purpose disclosed when the information is provided, and for any other purpose with your consent.

### *No Sales of Personal Information*

We do not sell any types of Personal Information to third parties, including as “sale” is defined in the California Consumer Privacy Act of 2018 (the “CCPA”), and we will not do so in the future without separately obtaining your consent.

### **Accessing, Correcting and Deleting Your Information**

#### *Requests to Know and Requests to Delete*

You may request that we disclose to you and provide a portable copy of the Personal Information about you that we have collected or that we maintain (a “Request to Know”), and you may request that we delete your Personal Information that we have collected or that we maintain (a “Request to Delete”). You may submit a Request to Know or Request to Delete by opening the Application on your mobile device, navigating to “My Account” and then selecting either the “Download My Data” option (for a Request to Know) or the “Purge My Info & Delete My Account” option (for a Request to Delete). Using the “Purge My Info & Delete My Account” feature will result in the permanent and irreversible deletion of your information and termination of your account on the Application. You may also submit a Request to Know or Request to Delete by e-mailing us at [privacyrequests@ivy.ai](mailto:privacyrequests@ivy.ai). Please note that if you submit your request via e-mail (or if you submit your request in any other manner) we will respond by providing you with the above instructions for using the “Download My Data” and “Purge My Info & Delete My Account” options within the Application.

Upon receipt of your Request to Know (“Download My Data”) or Request to Delete (“Purge My Info & Delete My Account”) through the Application as described above, we will take steps to verify your identity in order to confirm that the person making the request is actually the person about whom we have collected Personal Information (i.e., that the “you” making the request is actually you). We use the following steps to verify your identity and confirm your request:

- If you have registered to use the Application using your e-mail address, we will verify your identity and confirm your request by (1) sending you an e-mail to the e-mail address you used to register with the Application and (2) asking you to click the verification link in that e-mail.

- If you have registered to use the Application using your mobile telephone number, we will verify your identity and confirm your request by (1) sending you a verification code via SMS text message to the mobile telephone number you used to register with the Application and (2) asking you to enter that verification code into the Application.

If you have not yet registered to use our Application, please note that we have only limited information about you, and we may not have any Personal Information about you, so it is possible that we may be unable to reasonably verify your request.

We will use reasonable endeavors to accommodate verifiable Requests to Know and Requests to Delete submitted in the manner described above within a reasonable timeframe after receiving such requests. In any event, we will comply with your Request to Know and Request to Delete to the extent and in the manner required by applicable law in your jurisdiction, but we may deny a request, in whole or in part, to the extent an exception applies under (or as otherwise permitted by) applicable law in your jurisdiction. For example, we cannot and will not comply with a Request to Know or a Request to Delete if we cannot reasonably verify your identity in connection with your request.

You may also designate an authorized agent to make a Request to Know or Request to Delete on your behalf. An authorized agent may submit a Request to Know or Request to Delete on your behalf by e-mailing us at [privacyrequests@ivy.ai](mailto:privacyrequests@ivy.ai). If a duly-designated authorized agent makes a Request to Know or Request to Delete on your behalf, we will still require you to use the steps described above and to verify your own identity using the process described above, unless an exception applies under applicable law in your jurisdiction.

Due to the measures we have in place that are designed to maintain the security, confidentiality and integrity of your information on our systems, we generally cannot accommodate requests to access or delete your information except in the manner described above.

#### *Correcting Information*

You may send us an email at [team@ivy.ai](mailto:team@ivy.ai) to request a correction to any of your information that is inaccurate. We will evaluate such requests on a case-by-case basis. We may not accommodate a request to change information if we believe the change would violate any law or legal requirement, cause the information to be incorrect, or undermine our measures for maintaining the security, confidentiality and integrity of your information.

#### *No Differential Treatment*

If you choose to make a Request to Know or Request to Delete, or otherwise exercise your rights in relation to your Personal Information under applicable law in your jurisdiction, please know that you will not receive differential treatment by us as a result (e.g., different prices or quality of services), except to the limited extent permitted by applicable law.

#### **California “Shine The Light” Disclosure**

The California Civil Code permits California residents with whom we have an established business relationship to request that we provide a list of certain categories of Personal Information that we have disclosed to third parties for their direct marketing purposes during the preceding calendar year. To make such a request, please send an email to [team@ivy.ai](mailto:team@ivy.ai) or otherwise contact us using the information set forth below. Please mention that you are making a “California Shine the Light” inquiry. Please note, however, that we do not currently disclose Personal Information to third parties for their direct marketing purposes.

### **Users Outside of the United States**

Our Application is hosted in the United States and is provided from the United States. The Application is not intended to be used by individuals located outside of the United States at this time. If you are a resident of any country other than the United States, please note that by providing your Personal Information to us, you are consenting to the transfer of your Personal Information to the United States and other jurisdictions and to our use and disclosure of your Personal Information in accordance with this Policy.

### **Children Under the Age of 16**

Our Application is not intended for children under 16 years of age, and no one under the age of 16 may provide any information to us or others on or using our Application. We do not knowingly collect Personal Information from children under the age of 16. If you are under 16 years of age, do not use our Application or provide any information about yourself to us. If we learn we have collected or received Personal Information from a child under 16 years of age without verification of parental consent, we will delete that information. If you believe we might have any information from or about a child under the age of 16, please contact us at [team@ivy.ai](mailto:team@ivy.ai).

### **Data Security**

We have implemented measures designed to secure your Personal Information from accidental loss and from unauthorized access, use, alteration and disclosure. All information that you provide to us is stored on our servers behind firewalls, and certain Personal Information will be encrypted using secure socket layer (SSL) technology.

The safety and security of your information also depends on you. When we have given you (or when you have chosen) a password for access to certain parts of our Application, you are responsible for keeping that password confidential. We ask you not to share your password with anyone. Unfortunately, the transmission of information over the Internet is not completely secure. Although we have implemented security measures that we think are adequate, we cannot guarantee the security of your Personal Information transmitted to or using our Application. Any transmission of Personal Information is at your own risk. We are not responsible for the circumvention of any privacy settings or security measures contained on our Application.

### **Changes to Our Privacy Policy**

We post any changes we make to our Policy on this page. If we make material changes to how we treat Personal Information, we will notify you through a notice on the Application home page. The date this Policy was last revised is identified at the top of the page. You are responsible for periodically visiting our Application and this Policy to check for any changes.

### **Contact Information**

“We” are **IVY.AI, INC.**, a Delaware corporation with headquarters in Boulder, Colorado. To ask questions or to submit comments about this Policy and our privacy practices, you may contact us:

- Via E-mail: [team@ivy.ai](mailto:team@ivy.ai)
- Via Telephone: 805-864-2670
- Via Postal Mail: P.O. Box 1127, Boulder, CO 80306
- Via our Contact Us Page: <https://ivy.ai/contact-us>